Federal Digital System (FDsys) Requirements Document (RD) For Public Release

Revision 3.2 (RD-3.2)
Document Control Number (DCN): 7028518
4 December 2007

REVISION RECORD

REVISION	DATE	DESCRIPTION
Rev 3.2	4 Dec. 2007	Update incorporating Release 1C updates from Requirement Working Group sessions File: FDsys_Req_Doc_Public_Release_4Dec2007.doc
Rev 3.1	June 7, 2007	Updates based on refinement of requirement set
Rev 3.0	October 18, 2006	Updates based on refinement of requirement set
Rev 2.1	April 18, 2006	Format and correction updates
Rev 2.0	March 31, 2006	Updates based on refinement of requirement set
Rev 1.0	May 18, 2005	Version 1.0, initial issue

TABLE OF CONTENTS

Paragraph **Title** **Page**

1 INTRODUCTION

1.1 OVERVIEW

This document provides the requirement set for the Federal Digital System (FDsys) being developed and implemented by the U.S. Government Printing Office (GPO).

1.2 SYSTEM MISSION AND OBJECTIVES

By law and tradition, the GPO has three essential missions:

- To provide the three branches of the Federal Government with expert publishing and printing services.
- To provide perpetual, free and ready public access to the printed and electronic information published by the Federal Government in partnership with Federal Depository libraries.
- To distribute, on a cost recovery basis, printed and electronic copies of information published by the Federal Government.

Challenges to meeting this mission including:

- Access to government published information is now widely expected to be electronic.
- Digital information needs to be authentic and verified to be the correct version.
- Digital information needs to be available for access almost immediately.
- Information needs to be preserved, making it available for generations to come.

FDsys is being developed to contribute to meeting mission objectives in the following ways:

- FDsys will automate the collection and dissemination of electronic information from all three branches of government.
- Electronic markings will indicate that the information is authentic and will identify versions of documents that have been revised.
- Information will be permanently available in electronic format.
- Information will be accessible for Web searching, viewing, downloading and printing.
- Document masters will also be available for conventional and on-demand printing.

1.3 SYSTEM DESCRIPTION

FDsys will be a comprehensive, systematic, and dynamic means to create, ingest, authenticate, preserve, manage, and provide access to Government information from all three branches of the Federal Government. The system will automate and integrate lifecycle processes of Government information and deliver that information in formats suited to customer needs and desires.

FDsys will be built to include all known Federal Government publications falling within the scope of GPO's Federal Depository Library Program (FDLP), including text, graphics, video, audio, numeric, and other emerging forms of content. The full body of these publications will be available for searching, viewing, download, and printing, and will also be available for the production of document masters for conventional and on-demand printing.

System Releases: FDsys is being implemented in a series of incremental releases, each of which builds on those preceding it, and add improvements to system capability and underlying infrastructure.

Requirements: The requirements documented here are the product of a development process that has as its basis the FDsys Concept of Operations (ConOps) (rev. 2006) and previous versions of this document.

The requirements set is organized by Feature Groups, and then by Features within that Feature Group. Each requirement is assigned to a system release to designated the point in time for its implementation. In many instances, a ranking of criticality to that release is indicated. A designation of "Must" indicates a requirement essential to the successful function of the system at the time of that release. A designation of "Should" denotes functionality users will expect, and which should be implemented at that release in as many cases as possible. A designation of "Could" indicates functionality that, although desirable, is not viewed as critical to system function or user experience at the time of the release indicated.

2 REFERENCED DOCUMENTS

The following documents provide additional context for the development of FDsys, and are available at the GPO website (www.gpo.gov):

Concept of Operations (CONOPS) for the Future Digital System (FDsys), Version 2.0, 16 May 2005

GPO's Federal Digital System: System Releases And Capabilities, Version 5.0, FDsys Reference Document, December 19, 2007

3 FDSYS REQUIREMENTS

3.1 ACCESS FEATURE GROUP REQUIREMENTS

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2452	FDsys software applications and operating systems shall be Section 508 compliant according to 36 CFR Part 1194.21.	Access	508 Compliant User Interfaces	R2 Should
RD-2453	When software is designed to run on a system that has a keyboard, product functions shall be executable from a keyboard where the function itself or the result of performing a function can be discerned textually.	Access	508 Compliant User Interfaces	R2 Should / R3 Must
RD-2454	Applications shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards. Applications also shall not disrupt or disable activated features of any operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer.	Access	508 Compliant User Interfaces	R2 Should / R3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2455	An on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes.	Access	508 Compliant User Interfaces	R2 Should / R3 Must
RD-2456	The focus shall be programmatically exposed so that assistive technology can track focus and focus changes.	Access	508 Compliant User Interfaces	R2 Should / R3 Must
RD-2457	Sufficient information about a user interface element including the identity, operation and state of the element shall be available to assistive technology. When an image represents a program element, the information conveyed by the image shall also be available in text.	Access	508 Compliant User Interfaces	R2 Should / R3 Must
RD-2458	When images are used to identify controls, status indicators, or other programmatic elements, the meaning assigned to those images shall be consistent throughout an application's performance.	Access	508 Compliant User Interfaces	R2 Should / R3 Must
RD-2459	Textual information shall be provided through operating system functions for displaying text. The minimum information that shall be made available is text content, text input caret location, and text attributes.	Access	508 Compliant User Interfaces	R2 Should / R3 Must
RD-2460	Applications shall not override user selected contrast and color selections and other individual display attributes.	Access	508 Compliant User Interfaces	R2 Should / R3 Must
RD-2461	When animation is displayed, the information shall be displayable in at least one non-animated presentation mode at the option of the user.	Access	508 Compliant User Interfaces	R2 Should / R3 Must
RD-2462	Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	Access	508 Compliant User Interfaces	R2 Should / R3 Must
RD-2463	When a product permits a user to adjust color and contrast settings, a variety of color selections capable of producing a range of contrast levels shall be provided.	Access	508 Compliant User Interfaces	R2 Should / R3 Must
RD-2464	Software shall not use flashing or blinking text, objects, or other elements having a flash or blink frequency greater than 2 Hz and lower than 55 Hz.	Access	508 Compliant User Interfaces	R2 Should / R3 Must
RD-2465	When electronic forms are used, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.	Access	508 Compliant User Interfaces	R2 Should / R3 Must
RD-2468	Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.	Access	508 Compliant User Interfaces	R1C4 Must
RD-2471	Redundant text links shall be provided for each active region of a server-side image map.	Access	508 Compliant User Interfaces	R1C4 Must
RD-2472	Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.	Access	508 Compliant User Interfaces	R1C4 Must
RD-2476	Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.	Access	508 Compliant User Interfaces	R1C4 Must
RD-3799	The system shall provide public user GUIs that allow users to browse content by topic (i.e., subject).	Access	Browse Content	R1C4 Must
RD-3804	The system shall provide a public user GUIs that allow users to browse content by descriptive metadata elements.	Access	Browse Content	R1C4 Must
RD-2445	The system shall provide the capability to automatically transform content to create new renditions that are compliant with section 508 technical standards.	Access	Checking / Reformatting Content for 508 Compliance	R2 Must
RD-2446	The system shall provide the capability to validate content for compliance with Section 508 technical standards.	Access	Checking / Reformatting Content for 508 Compliance	R2 Must
RD-2447	The system shall accept accessibility requirements and implementation guidance from Content Originators.	Access	Checking / Reformatting Content for 508 Compliance	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2449	In order to achieve compliance with Section 508 technical standards, established best practices shall be followed.	Access	Checking / Reformatting Content for 508 Compliance	R2 Could
RD-2450	The system shall create content that contains well formed code which conforms to World Wide Web Consortium (W3C) Guidelines.	Access	Checking / Reformatting Content for 508 Compliance	R2 Must
RD-3792	The system shall provide the capability for authorized users to flag content for a manual section 508 accessibility check.	Access	Checking / Reformatting Content for 508 Compliance	R1C4 Must
RD-471	The system shall have the capability to automatically perform 508 accessibility assessments on content.	Access	Checking / Reformatting Content for 508 Compliance	R2 Must
RD-3213	The system shall enable GPO users to view and manage contact data while not connected to the internet or internal server.	Access	Contact Management	R2 Must
RD-3214	The system shall have the capability to synchronize data managed offline with the contact database when reconnected.	Access	Contact Management	R2 Must
RD-3215	The system shall enable GPO users to track contact data (e.g., name, company, address, phone, e-mail, last meeting date, and status).	Access	Contact Management	R2 Must
RD-3216	The system shall enable GPO users to create customizable fields for contact data (e.g., billing address code, GPO Express Customer).	Access	Contact Management	R2 Must
RD-3217	The system shall enable GPO users to manage notes, history, sales, and attached files to each contact record.	Access	Contact Management	R2 Must
RD-3218	The system shall allow each contact to have an owner associated with the contact record.	Access	Contact Management	R2 Must
RD-3219	The system shall enable GPO users to manage groups of related contact records (e.g., all contacts at a single agency).	Access	Contact Management	R2 Must
RD-3220	The system shall enable GPO users to hierarchically group contact records.	Access	Contact Management	R2 Must
RD-3221	The system shall enable GPO users to track sales opportunities via contact data.	Access	Contact Management	R2 Must
RD-3222	The system shall enable GPO users to generate sales opportunities reports via contact data.	Access	Contact Management	R2 Must
RD-3223	The system shall have the capability to integrate a contact management tool with GPO's e-mail client (e.g., Microsoft Outlook).	Access	Contact Management	R2 Must
RD-3224	The system shall have the capability to integrate a contact management tool with handheld devices used by GPO employees (e.g., Blackberry devices).	Access	Contact Management	R2 Must
RD-3225	The contact management tool shall have a calendar which synchronizes with GPO's e-mail client calendar.	Access	Contact Management	R2 Must
RD-3226	The contact management tool shall enable GPO users to schedule calls, meetings and tasks associated with each contact record.	Access	Contact Management	R2 Must
RD-3227	The contact management tool shall enable users to prioritize tasks.	Access	Contact Management	R2 Must
RD-3228	The system shall enable GPO users to generate mail merges using information stored in contact records.	Access	Contact Management	R2 Must
RD-3229	The system shall enable GPO users to search contact records with any field.	Access	Contact Management	R2 Must
RD-3230	The system shall enable GPO users to search contact records for empty fields or non-empty fields.	Access	Contact Management	R2 Must
RD-3231	The contact management tool shall enable authorized users to generate reports.	Access	Contact Management	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3232	The system shall enable GPO users to create customized report templates/layouts for reports generated by the contact management tool.	Access	Contact Management	R2 Must
RD-3233	The system shall allow users to record and store meeting minutes with internal and external contacts.	Access	Contact Management	R2 Could
RD-3234	The system shall allow users to associate multiple internal and external contacts with the meeting minutes.	Access	Contact Management	R2 Could
RD-3235	The system shall allow users to associate meeting minutes with a list of hierarchical categories in the contact management tool	Access	Contact Management	R2 Could
RD-3236	The system shall allow users to record the date, time, location and subject of the meeting in the contact management tool.	Access	Contact Management	R2 Could
RD-3237	The system shall allow users to record the content of the meeting in the contact management tool using an unlimited number of characters.	Access	Contact Management	R2 Could
RD-3238	The system shall allow users to generate reports in the contact management tool that include details of all meeting minutes.	Access	Contact Management	R2 Could
RD-3239	The system shall allow users to filter the data for reports generated by the contact management tool by contact, department, and category.	Access	Contact Management	R2 Could
RD-3241	The system shall provide the capability for users to generate reports from the contact management tool that contain the meeting subject.	Access	Contact Management	R2 Could
RD-3242	The system shall provide the capability for users to generate reports from the contact management tool that contain a list of all contacts associated with the meeting.	Access	Contact Management	R2 Could
RD-3243	The system shall provide the capability for users to generate reports from the contact management tool that contain date, time, and location of meeting.	Access	Contact Management	R2 Could
RD-3244	The system shall provide the capability for users to generate reports from the contact management tool that contain full meeting minutes.	Access	Contact Management	R2 Could
RD-3245	The system shall provide the capability for users to generate reports from the contact management tool that contain a list of all categories associated with the meeting	Access	Contact Management	R2 Could
RD-2341	The system shall provide the capability to link Congressional bill citations in content to corresponding versions of publicly available Congressional bill renditions.	Access	Create Persistent Links	R1C4 Must
RD-2342	The system shall provide the capability to link public law citations in digital objects to corresponding versions of publicly available public law renditions.	Access	Create Persistent Links	R1C4 Must
RD-2343	The system shall provide the capability to link United States Code citations in content to corresponding versions of publicly available United States Code rendition granules.	Access	Create Persistent Links	R1C4 Must
RD-2344	The system shall provide the capability to link Statutes at Large citations in content to corresponding versions of publicly available Statutes at Large rendition granules.	Access	Create Persistent Links	R1C4 Must
RD-2345	The system shall provide the capability to link Code of Federal Regulations citations in content to corresponding versions of publicly available Code of Federal Regulations rendition granules.	Access	Create Persistent Links	R1C4 Must
RD-2347	The system shall provide the capability to link Congressional Record page number citations in content to corresponding versions of publicly available Congressional Record pages in rendition granules.	Access	Create Persistent Links	R1C4 Must
RD-2349	The system shall provide the capability to link Federal Register page number citations in content to corresponding versions of publicly available Federal Register pages in rendition granules.	Access	Create Persistent Links	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2353	The system shall provide the capability to link Congressional Report citations in content to corresponding versions of publicly available Congressional Report renditions.	Access	Create Persistent Links	R1C4 Must
RD-2357	The system shall provide the capability to manage links as managed objects.	Access	Create Persistent Links	R1C4 Must
RD-3746	The system shall provide the capability to link member of Congress names in content to the corresponding version of a publicly available rendition granule of a target publication that is based on the source publication.	Access	Create Persistent Links	R1C4 Must
RD-3747	The system shall provide the capability to link entities in the Congressional Record Index to the entries in the corresponding versions of publicly available Congressional Record rendition granules.	Access	Create Persistent Links	R1C4 Must
RD-3748	The system shall provide the capability to link Weekly Compilation of Presidential Documents citations in content to corresponding versions of publicly available Weekly Compilation of Presidential Documents rendition granules.	Access	Create Persistent Links	R1C4 Must
RD-3749	The system shall provide the capability to link Congressional Calendar citations in content to corresponding versions of publicly available Congressional Calendar rendition granules.	Access	Create Persistent Links	R1C4 Must
RD-3750	The system shall provide the capability to link related RIN numbers in the Unified Agenda to corresponding versions of publicly available Unified Agenda rendition granules.	Access	Create Persistent Links	R1C4 Must
RD-3751	The system shall provide the capability to link RIN Numbers in the Unified Agenda to corresponding versions of publicly available Federal Register rendition granules.	Access	Create Persistent Links	R1C4 Must
RD-3295	The system shall have the capability to push DIPs to users using an RSS feeds conforming to the RSS 2.0 Specification.	Access	Deliver by RSS	R1C4 Must
RD-3296	The system shall have the capability for users to sign up to receive DIPS via RSS feed for new publications added to GPO defined collections.	Access	Deliver by RSS	R1C4 Must
RD-3297	The system shall have the capability for users to sign up to receive DIPS via RSS feed for new publications added by user defined criteria.	Access	Deliver by RSS	R2 Must
RD-3318	The maximum size DIP delivered by RSS feed shall be configurable by an authorized user.	Access	Deliver by RSS	R1C4 Must
RD-118	The system shall provide the capability to deliver packaged DIPs that contain only metadata expressed in schemas supported by the schema registry.	Access	Deliver Content and/or Metadata	R2 Must
RD-124	The system shall provide the capability for batch delivery of content and metadata together from multiple publications.	Access	Deliver Content and/or Metadata	R2 Must
RD-125	The system shall provide the capability for batch delivery of metadata from multiple publications.	Access	Deliver Content and/or Metadata	R2 Must
RD-126	The system shall provide the capability for batch delivery of content from multiple publications.	Access	Deliver Content and/or Metadata	R2 Must
RD-2270	The system shall provide the capability for users to access content that has been published in non-English languages and non-Roman character sets.	Access	Deliver Content and/or Metadata	R3 Must
RD-2425	The system shall provide the capability for access processing to provide content and/or metadata and/or business process information to delivery processing for the purpose of fulfilling an End User request or Content Originator order.	Access	Deliver Content and/or Metadata	R2 Must
RD-2428	The system shall provide business process information to delivery processing for the purpose of fulfilling an End User request.	Access	Deliver Content and/or Metadata	R2 Must
RD-2429	The system shall provide content, metadata and business process information in any combination to delivery processing for the purpose of fulfilling an End User request.	Access	Deliver Content and/or Metadata	R2 Must
RD-2433	The system shall provide content, metadata and business process information in any combination to delivery processing for the purpose of fulfilling an Content Originator order.	Access	Deliver Content and/or Metadata	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2434	The system shall provide the capability to perform records management functions on ACPs.	Access	Deliver Content and/or Metadata	R2 Must
RD-2435	Records management functions shall comply with GPO and Federal records management policies.	Access	Deliver Content and/or Metadata	R2 Must
RD-2436	Records management functions shall be performed according to records management schedules for content and metadata within the system.	Access	Deliver Content and/or Metadata	R2 Must
RD-2775	The system shall provide the capability for Federal Depository Library End Users to select and request content and metadata for delivery to their library based on their unique profile and preferences.	Access	Deliver Content and/or Metadata	R2 Must
RD-2776	The system shall comply with GPO policies related to selection of tangible and electronic titles by Federal Depository Library End Users.	Access	Deliver Content and/or Metadata	R2 Must
RD-2777	The system shall provide the capability to interface with Authorized Representatives designated by GPOs Library Services and Content Management business unit for processing of no-fee delivery requests.	Access	Deliver Content and/or Metadata	R2 Must
RD-2778	The system shall provide the capability to interface with GPO's Integrated Library System and other legacy systems as defined by GPO business units for processing of no-fee requests.	Access	Deliver Content and/or Metadata	R2 Must
RD-2779	The system shall provide the capability to process no-fee requests for delivery of content with access restrictions.	Access	Deliver Content and/or Metadata	R2 Must
RD-2780	The system shall support the delivery of serials and periodicals.	Access	Deliver Content and/or Metadata	R2 Must
RD-2782	The system shall provide the capability for users to cancel full requests prior to fulfillment.	Access	Deliver Content and/or Metadata	R2 Must
RD-2783	The system shall provide the capability for users to cancel partial requests prior to fulfillment.	Access	Deliver Content and/or Metadata	R2 Must
RD-2784	The system shall provide the capability to deliver personalized offers to registered users based on user request history or users with similar request histories. (e.g. "you may also be interested in…").	Access	Deliver Content and/or Metadata	R2 Must
RD-2785	The system shall provide the capability for users to opt-out of personalized offers.	Access	Deliver Content and/or Metadata	R2 Must
RD-2786	The system shall provide the capability to provide authorized users with a content delivery packing list	Access	Deliver Content and/or Metadata	R1C4 Must
RD-2788	The system shall provide the capability to provide public users with a content delivery packing list.	Access	Deliver Content and/or Metadata	R2 Must
RD-2790	The system shall provide the capability for users to request fee-based content delivery.	Access	Deliver Content and/or Metadata	R2 Must
RD-2791	The system shall have the capability to interface with external Authorized Representatives as designated by GPO's Publication and Information Sales business unit for processing of fee-based delivery requests.	Access	Deliver Content and/or Metadata	R2 Must
RD-2792	The system shall provide the capability to interface with GPO's financial and inventory systems for processing of fee-based requests.	Access	Deliver Content and/or Metadata	R2 Must
RD-2793	The system shall have the capability to retrieve price information from external systems.	Access	Deliver Content and/or Metadata	R2 Must
RD-2794	The system shall have the capability to adjust price information for fee-based content delivery.	Access	Deliver Content and/or Metadata	R2 Must
RD-2795	Pricing structures shall comply with GPO's legislative mandates under Title 44 of the United States Code and GPO's Sales Program policies.	Access	Deliver Content and/or Metadata	R2 Must
RD-2796	The system shall provide the capability for authorized users to manually adjust the price.	Access	Deliver Content and/or Metadata	R2 Must
RD-2797	The system shall provide the capability to dynamically adjust the price.	Access	Deliver Content and/or Metadata	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2798	The system shall provide the capability to apply price schedules.	Access	Deliver Content and/or Metadata	R2 Must
RD-2799	The system shall adhere to industry best practices for performance of a Web-accessible e-commerce system.	Access	Deliver Content and/or Metadata	R2 Must
RD-2800	The system shall include an online bookstore web interface that complies with the FDsys interface requirements and includes a shopping cart, order tracking, backorder capabilities, third party ordering, thumbnail cover images, and a fully browseable and searchable catalog of items available for purchase that is updated at least daily.	Access	Deliver Content and/or Metadata	R2 Must
RD-2801	The system shall provide the capability to process international and domestic requests for hard copy, electronic presentation, digital media, and service product lines as designated by GPO's Publication and Information Sales business unit.	Access	Deliver Content and/or Metadata	R2 Must
RD-2802	The system shall provide the capability to process fee-based requests for the delivery of content with access restrictions.	Access	Deliver Content and/or Metadata	R2 Must
RD-2803	The system shall support the collection of information (order taking) and pass this information to external systems for processing.	Access	Deliver Content and/or Metadata	R2 Must
RD-2805	The system shall support the collection of payment information via check/electronic transfer.	Access	Deliver Content and/or Metadata	R2 Must
RD-2806	The system shall support the collection of payment information via Major credit cards including Visa, MasterCard, Discover/NOVUS, and American Express.	Access	Deliver Content and/or Metadata	R2 Must
RD-2807	The system shall support the collection of payment information via debit cards.	Access	Deliver Content and/or Metadata	R2 Must
RD-2808	The system shall support the collection of payment information via purchase orders.	Access	Deliver Content and/or Metadata	R2 Must
RD-2809	The system shall support the collection of payment information via requests for invoicing.	Access	Deliver Content and/or Metadata	R2 Must
RD-2810	The system shall support the collection of payment information via deposit accounts.	Access	Deliver Content and/or Metadata	R2 Must
RD-2811	The system shall support the collection of payment information via government account.	Access	Deliver Content and/or Metadata	R2 Must
RD-2812	The system shall support the collection of payment information via cash.	Access	Deliver Content and/or Metadata	R2 Must
RD-2813	The system shall support the collection of payment information via gift card.	Access	Deliver Content and/or Metadata	R2 Must
RD-2814	The system shall securely pass information to external systems for processing.	Access	Deliver Content and/or Metadata	R2 Must
RD-2815	The system shall comply with the Federal Trade Commission's Mail or Telephone Order Merchandise Rule.	Access	Deliver Content and/or Metadata	R2 Must
RD-2816	The system shall comply with the Fair Credit Billing Act.	Access	Deliver Content and/or Metadata	R2 Must
RD-2817	The system shall comply with the Fair Credit Reporting Act.	Access	Deliver Content and/or Metadata	R2 Must
RD-2818	The system shall comply with the Children's Online Privacy Protection Act (COPPA).	Access	Deliver Content and/or Metadata	R2 Must
RD-2819	The system shall comply with the FTC's rules for implementing the Children's Online Privacy Protection Act (COPPA).	Access	Deliver Content and/or Metadata	R2 Must
RD-2820	The system shall provide the capability to automatically verify and validate payment information submitted by users prior to delivery fulfillment.	Access	Deliver Content and/or Metadata	R2 Must
RD-2821	The system shall provide the capability to validate payment information in real-time via external GPO systems.	Access	Deliver Content and/or Metadata	R2 Must
RD-2822	The system shall provide the capability to validate payment information in real-time via the U.S. Treasury Department's Pay.gov credit card processing system	Access	Deliver Content and/or Metadata	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2823	The system shall provide the capability for users to delegate requests to other users (e.g. user's "hand-off" orders to other authorized officials to submit payment).	Access	Deliver Content and/or Metadata	R2 Must
RD-2825	The system shall provide the capability to display lists of all hard copy, electronic presentation, digital media, and service product lines as designated by GPO's Publication and Information Sales business unit.	Access	Deliver Content and/or Metadata	R2 Must
RD-2826	The system shall support delivery of content by subscriptions (i.e. an agreement by which a user obtains access to requested content by payment of a periodic fee or other agreed upon terms.)	Access	Deliver Content and/or Metadata	R2 Must
RD-2827	The system shall provide the capability to manage, secure, and maintain End User information associated with subscriptions.	Access	Deliver Content and/or Metadata	R2 Must
RD-2831	The system shall provide the capability for users to cancel full or partial requests prior to fulfillment.	Access	Deliver Content and/or Metadata	R2 Must
RD-2832	The system shall provide the capability to provide authorized users with a detailed transaction summary.	Access	Deliver Content and/or Metadata	R2 Must
RD-2833	The system shall provide the capability for authorized users to configure transaction summaries.	Access	Deliver Content and/or Metadata	R2 Must
RD-2834	The system shall provide the capability to manage transaction records according to GPO, Federal, and FTC regulations in accordance with GPO privacy and required records retention policies.	Access	Deliver Content and/or Metadata	R2 Must
RD-2835	The system shall securely maintain electronic copies of orders, shipments, and financial records for at least seven years.	Access	Deliver Content and/or Metadata	R2 Must
RD-2836	The system shall provide the capability to generate reports for fee-based transactions (e.g., order histories, sales transactions, inventory data).	Access	Deliver Content and/or Metadata	R2 Must
RD-2838	The system shall have the capability to determine what options are available for delivery of particular content or metadata.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-2839	The system shall provide the capability for users to request delivery of content or metadata from available options as defined by GPO business units.	Access	Deliver Content and/or Metadata	R2 Must
RD-2841	The system shall provide the capability for users to select file type from available options (e.g., DOC, MP3, PDF).	Access	Deliver Content and/or Metadata	R1C4 Must
RD-2842	The system shall provide the capability for users to select resolution (e.g., images, video) from available options.	Access	Deliver Content and/or Metadata	R2 Must
RD-2843	The system shall provide the capability for users to select color space from available options (e.g. RGB, CMYK).	Access	Deliver Content and/or Metadata	R2 Must
RD-2844	The system shall provide the capability for users to select compression and size from available options.	Access	Deliver Content and/or Metadata	R2 Must
RD-2845	The system shall provide the capability for users to select transfer rate from available options.T	Access	Deliver Content and/or Metadata	R2 Must
RD-2846	The system shall provide the capability for users to select platform from available options.	Access	Deliver Content and/or Metadata	R2 Must
RD-2848	The system shall provide the capability for users to select delivery of related content from available options.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-2850	The system shall provide the capability for users to select quantity of items requested for delivery (e.g., one, five, batch).	Access	Deliver Content and/or Metadata	R1C4 Must
RD-2851	The system shall provide the capability for users to select output type from available options (e.g., hard copy, electronic presentation, digital media).	Access	Deliver Content and/or Metadata	R1C4 Must
RD-2852	The system shall provide the capability for users to select data storage device from available options (e.g., CD, DVD, server).	Access	Deliver Content and/or Metadata	R1C4 Must
RD-2855	The system shall provide the capability for users to schedule delivery from the system.	Access	Deliver Content and/or Metadata	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2856	The system shall provide the capability for users to select tangible delivery method from available options (e.g., air transportation, ground transportation, pickup, overnight, priority, freight).	Access	Deliver Content and/or Metadata	R2 Must
RD-2857	The system shall provide the capability for GPO to offer users separate "bill to" and "ship to" options for delivery or shipment of tangible content.	Access	Deliver Content and/or Metadata	R2 Must
RD-2858	The system shall provide the capability for users to submit multiple address options for delivery or shipment of tangible content.	Access	Deliver Content and/or Metadata	R2 Must
RD-2859	The system shall provide the capability to preview requested content.	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-2861	The system shall provide the capability for authorized users to preview publications that have been created from custom composition and content formatting.	Access	Deliver Content and/or Metadata	R3 Must
RD-2862	The system shall have the capability to support custom composition and content formatting from available options (e.g., 2 columns, cover stock, font).	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-2865	The system shall provide the capability to assign an order number for requests.	Access	Deliver Content and/or Metadata	R2 Must
RD-2866	The system shall not repeat an order number.	Access	Deliver Content and/or Metadata	R2 Must
RD-2868	The system shall have the capability to provide order numbers to users.	Access	Deliver Content and/or Metadata	R2 Must
RD-2869	The system shall provide the capability for users to track the status of their requests.	Access	Deliver Content and/or Metadata	R2 Must
RD-2898	The system will provide for the delivery of output in a variety user-specified methods or formats, including electronic mail or Web pages.	Access	Deliver Content and/or Metadata	R2 Must
RD-2899	The system will be capable of delivering metadata to users in electronic mail messages.	Access	Deliver Content and/or Metadata	R2 Must
RD-2900	The system will be capable of delivering metadata to users in Web pages.	Access	Deliver Content and/or Metadata	R2 Must
RD-2901	The system shall support the capability to deliver metadata to users in additional formats in the future.	Access	Deliver Content and/or Metadata	R2 Must
RD-2902	The system shall output metadata in formats specified by the user, including MARC, ONIX, ASCII text, or comma delimited text.	Access	Deliver Content and/or Metadata	R2 Must
RD-2903	The system shall output metadata in MARC format when requested by the user.	Access	Deliver Content and/or Metadata	R2 Must
RD-2904	The system shall output metadata in ONIX format when requested by the user.	Access	Deliver Content and/or Metadata	R2 Must
RD-2905	The system shall output metadata in ASCII text format when requested by the user.	Access	Deliver Content and/or Metadata	R2 Must
RD-2906	The system shall output metadata in comma-delimited format when requested by the user.	Access	Deliver Content and/or Metadata	R2 Must
RD-2907	The system shall support the capability to output metadata in additional formats in the future.	Access	Deliver Content and/or Metadata	R2 Must
RD-3257	The system shall support the capability for a user to pull a DIP from the system using additional methods in the future.	Access	Deliver Content and/or Metadata	R3 Must
RD-3266	The system shall have the capability to determine if delivery is possible based upon limitations of delivery mechanisms.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3267	The system shall have the capability to determine if delivery is possible based upon limitations of content formats.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3268	The system shall have the capability to inform users that delivery is not possible.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3269	The system shall have the capability to inform users why delivery is not possible.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3270	The system shall have the capability to provide users with estimated transfer time for delivery.	Access	Deliver Content and/or Metadata	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3284	The system shall have the capability to make adjustments to digital objects for delivery based on digital object format.	Access	Deliver Content and/or Metadata	R2 Must
RD-3285	The system shall have the capability to adjust the resolution of digital objects.	Access	Deliver Content and/or Metadata	R2 Must
RD-3286	The system shall have the capability to resize digital objects.	Access	Deliver Content and/or Metadata	R2 Must
RD-3287	The system shall have the capability to adjust the compression of digital objects.	Access	Deliver Content and/or Metadata	R2 Must
RD-3288	The system shall have the capability to adjust the color space of digital objects. (e.g., CMYK to RGB)	Access	Deliver Content and/or Metadata	R2 Must
RD-3289	The system shall have the capability to adjust the image quality settings of digital objects. (e.g., transparency, dithering, anti-aliasing)	Access	Deliver Content and/or Metadata	R2 Must
RD-3292	The system shall have the capability to repurpose content from multiple packages into a single DIP.	Access	Deliver Content and/or Metadata	R2 Must
RD-3306	The system shall support the capability to push DIPs to users using additional methods in the future.	Access	Deliver Content and/or Metadata	R3 Must
RD-3316	The maximum size DIP delivered by HTTP download shall be configurable by an authorized user.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3324	The maximum size DIP delivered by a future electronic channel shall be configurable by an authorized user.	Access	Deliver Content and/or Metadata	R3 Must
RD-3340	The system shall have the capability to support hard copy output for variable data printing processes.	Access	Deliver Content and/or Metadata	R3 Could
RD-3341	The system shall have the capability to add the GPO Imprint line to DIPs and pre-ingest bundles per the GPO Publication 310.2 and the New Imprint Line Announcement.	Access	Deliver Content and/or Metadata	R2 Could
RD-3342	The system shall allow users to manually add the Imprint line.	Access	Deliver Content and/or Metadata	R2 Could
RD-3343	The system shall automatically add the Imprint Line.	Access	Deliver Content and/or Metadata	R2 Could
RD-3344	The system shall allow users to manually adjust the location of the Imprint line.	Access	Deliver Content and/or Metadata	R2 Could
RD-3356	The system shall support the capability to deliver page layout files containing images, fonts, and linked text files in additional formats in the future.	Access	Deliver Content and/or Metadata	R3 Must
RD-3372	The system shall support the capability to deliver text files in additional file formats in the future.	Access	Deliver Content and/or Metadata	R3 Must
RD-3375	The system shall have the capability to generate DIPs and pre-ingest bundles that contain Job Definition Format (JDF) data.	Access	Deliver Content and/or Metadata	R3 Could
RD-3383	The system shall have the capability to render content for presentation on end user devices.	Access	Deliver Content and/or Metadata	R2 Must
RD-3388	The system shall have the capability to render content for presentation on non-desktop devices.	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-3389	The system shall have the capability to render content for presentation on Digital Assistants (PDAs).	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-3390	The system shall have the capability to render content for presentation on Digital Audio Players.	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-3391	The system shall have the capability to render content for presentation on Electronic Books (E-Books).	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-3392	The system shall have the capability to render content for presentation on Cell Phones.	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-3393	The system shall have the capability to determine and deliver the file format needed for non-desktop electronic devices.	Access	Deliver Content and/or Metadata	R2 Could
RD-3394	The system shall provide the capability to deliver DIPs that support static and dynamic text in multiple formats.	Access	Deliver Content and/or Metadata	R2 Must
RD-3404	The system shall have the capability to deliver electronic content in Open Document Format that is equivalent to the native file.	Access	Deliver Content and/or Metadata	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3407	The system shall have the capability to deliver electronic content in Microsoft Word Document File Format (.doc) that is equivalent to the original file as ingested.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3411	The system shall have the capability to deliver electronic content in Open eBook Publication Structure (OEBPS) in accordance with Open eBook Publication Structure Specification Version 1.2.	Access	Deliver Content and/or Metadata	R2 Could
RD-3413	The system shall have the capability to deliver electronic content in JPEG that is equivalent to the original file as ingested.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3419	The system shall provide the capability to deliver audio content.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3420	The system shall have the capability to deliver audio content in MPEG 1 - Audio Layer 3 (MP3) that is equivalent to the native file.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3421	The system shall have the capability to deliver audio content in FLAC (Free Lossless Audio Codec) that is equivalent to the native file.	Access	Deliver Content and/or Metadata	R2 Must
RD-3422	The system shall have the capability to deliver audio content in Ogg Vorbis that is equivalent to the native file.	Access	Deliver Content and/or Metadata	R2 Must
RD-3423	The system shall have the capability to deliver audio content in CDDA (Compact Disc Digital Audio) that is equivalent to the native file.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3424	The system shall provide the capability to deliver DIPs that support audiovisual content (e.g., video, multimedia) in MPEG format.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3426	The system shall deliver electronic content that maintains hyperlinks to the extent possible.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3440	The system shall have the capability to deliver DIPs that support the creation of Blue Ray Discs (BD).	Access	Deliver Content and/or Metadata	R3 Could
RD-3454	The system shall have the capability to generate image files that can be used to duplicate/replicate the content that will be stored on removable digital media.	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-3455	The system shall have the capability to generate ISO image files.	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-3456	The system shall have the capability to generate VCD image files.	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-3457	The system shall have the capability to generate UDF image files.	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-3468	The system shall have the capability to deliver DIPs to Digital Assistants (PDAs).	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-3469	The system shall have the capability to deliver DIPs to Digital Audio Players.	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-3470	The system shall have the capability to deliver DIPs to Electronic Books (E-Books).	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-3471	The system shall have the capability to deliver DIPs to Cell Phones.	Access	Deliver Content and/or Metadata	R2 Should / R3 Must
RD-3722	The system shall provide the capability to deliver packaged DIPs that contain only content that is stored in the system.	Access	Deliver Content and/or Metadata	R2 Must
RD-3726	The system shall provide the capability to deliver content from one or more renditions of a single publication.	Access	Deliver Content and/or Metadata	R2 Must
RD-3727	The system shall provide the capability to deliver content and metadata together from one or more renditions of a single publication.	Access	Deliver Content and/or Metadata	R2 Must
RD-3728	The system shall provide the capability for batch delivery of content from a single publication.	Access	Deliver Content and/or Metadata	R2 Must
RD-3729	The system shall provide the capability for batch delivery of metadata from a single publication.	Access	Deliver Content and/or Metadata	R2 Must
RD-3730	The system shall provide the capability for batch delivery of content and metadata from a single publication.	Access	Deliver Content and/or Metadata	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3731	The system shall provide the capability for batch delivery of content packages.	Access	Deliver Content and/or Metadata	R2 Must
RD-3735	The DIP shall have the capability to embed one or more metadata files associated with the content.	Access	Deliver Content and/or Metadata	R2 Must
RD-3736	The DIP shall have the capability to embed one or more digital objects associated with metadata.	Access	Deliver Content and/or Metadata	R2 Must
RD-3783	The system shall provide the capability for public users to select delivery of MARC XML via a link on the content detail GUI.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3784	The system shall provide the capability for public users to select delivery of Dublin Core via a link on the content detail GUI.	Access	Deliver Content and/or Metadata	R2 Must
RD-3785	The system shall provide the capability for public users to select delivery of ONIX via a link on the content detail GUI.	Access	Deliver Content and/or Metadata	R2 Must
RD-3791	The system shall have the capability to deliver electronic content in Microsoft Word Document File Format (.doc) that is equivalent to the original file as ingested.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-3794	The system shall have the capability to deliver content to a Linux platform.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-384	The system shall create a DIP in response to a user request.	Access	Deliver Content and/or Metadata	R2 Must
RD-388	The system shall copy content and metadata to a DIP from the publication's AIP when the information needed is not present in the ACP.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-391	The DIP shall have the capability to include transient copies of digital objects that are optimized for delivery from the system.	Access	Deliver Content and/or Metadata	R2 Must
RD-415	The system shall provide the capability to embed metadata files (e.g., MARC, ONIX, Dublin Core, MODS) as required to support delivery.	Access	Deliver Content and/or Metadata	R2 Must
RD-423	The system shall provide the capability to copy descriptive metadata in ONIX format to a DIP.	Access	Deliver Content and/or Metadata	R2 Must
RD-424	The system shall provide the capability to copy descriptive metadata in Dublin Core format to a DIP.	Access	Deliver Content and/or Metadata	R1C4 Must
RD-426	The system shall provide the capability to copy descriptive metadata in COSATI format to a DIP.	Access	Deliver Content and/or Metadata	R3 Must
RD-427	The system shall support the capability to copy additional descriptive metadata formats to the DIP in the future.	Access	Deliver Content and/or Metadata	R3 Must
RD-3298	The system shall provide capability to deliver a DIP to users via e-mail.	Access	Delivery By Email	R1C4 Must
RD-3299	The system shall provide the capability to deliver a batch of DIPs to users via e-mail.	Access	Delivery By Email	R1C4 Must
RD-3300	The system shall provide the capability to deliver a batch of DIPs to users at a frequency defined by GPO when new publications are added to a GPO defined collection.	Access	Delivery By Email	R1C4 Must
RD-3320	The system shall provide the capability for an authorized users to configure the maximum size of a DIP that is delivered via e-mail to users.	Access	Delivery By Email	R1C4 Must
RD-3264	The system shall have the capability to determine if delivery is possible.	Access	Delivery By Ftp	R2 Must
RD-3265	The system shall have the capability to determine if delivery is possible based upon business rules.	Access	Delivery By Ftp	R2 Must
RD-3304	Users shall have the capability to request that files be transferred via FTP to their server for a DIP based on user defined criteria.	Access	Delivery By Ftp	R1C4 Must
RD-3305	The system shall have the capability to push DIPs to users using Secure File Transfer Protocol.	Access	Delivery By Ftp	R3 Must
RD-3322	The maximum size DIP delivered by FTP shall be configurable by an authorized user.	Access	Delivery By Ftp	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3328	The time required to deliver via FTP a DIP created from an ACP that contains a 10 MB (TBS) set of files to an average PC (TBS) connected to the GPO Intranet running an FTP server shall be 60 seconds (TBS) or less.	Access	Delivery By Ftp	R3 Must
RD-3329	The time required to deliver via FTP a DIP created from an AIP in online storage that contains a 10 MB (TBS) set of files to an average PC (TBS) connected to the GPO Intranet running Internet Explorer 6 shall be 65 seconds (TBS) or less.	Access	Delivery By Ftp	R3 Must
RD-2271	The system shall provide the capability for users to access information about content relationships.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2277	The system shall provide information to users via a GUI that lists all of the versions of a bill that are available for access.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2280	The system shall provide the capability to access public laws based on public law citations in the House Calendar.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2281	The system shall provide the capability to access public laws based on public law citations in the Senate Calendar of Business.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2282	The system shall provide the capability to access Congressional bills based on bill citations in the House Calendar.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2283	The system shall provide the capability to access Congressional bills based on bill citations in the Senate Calendar of Business.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2284	The system shall provide the capability to access bill versions based on entries in the history of bills.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2285	The system shall provide the capability to access Congressional Record pages based on Congressional Record citations in the history of bills.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2286	The system shall provide the capability to access Congressional bills based on bill citations in the Congressional Record.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2287	The system shall provide the capability to access public laws based on public law citations in the history of bills.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2288	The system shall provide the capability to access history of bill granules based on bill citations in public laws.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2289	The system shall provide the capability to access Congressional Record granules based on Congressional Record citations in public laws.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2290	The system shall provide the capability to access U.S. Code granules based on U.S. Code citations in public laws.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2291	The system shall provide the capability to access public laws based on public law citations in the U.S. Code.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2293	The system shall provide the capability to access Congressional Reports based on Congressional Report citations in Congressional bills.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2294	The system shall provide the capability access to Congressional hearings related to Congressional bills.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2295	The system shall provide the capability to access granules in the Congressional Record based on entries in the Congressional Record Index.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2296	The system shall provide the capability to access Statutes at Large granules based on Statutes at Large citations in public laws.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2299	The system shall provide the capability to access Code of Federal Regulation sections based on Code of Federal Regulation citation in the Federal Register.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2300	The system shall provide the capability to access Federal Register granules based on Federal Register citations in the List of CFR Sections Affected.	Access	Follow Relationships To Other Documents	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2301	The system shall provide the capability to access Code of Federal Regulation sections based on Code of Federal Regulation citations in the List of CFR Sections Affected.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2302	The system shall provide the capability to access Code of Federal Regulation sections based on Code of Federal Regulation citations in the Unified Agenda.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2303	The system shall provide the capability to access content based on relationships between Supreme Court publications that are part of the opinion process.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2304	The system shall provide notification to users about related Supreme Court publications that are part of the opinion process.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2305	The system shall provide notification to users that informs them of the current version of an opinion.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2306	The system shall provide notification to users that informs them of superseded versions of an opinion.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2307	The system shall provide notification to users when a bench opinion has been superseded by a slip opinion.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2308	The system shall provide notification to users when a slip opinion has been superseded by a preliminary print of the U.S. Reports.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2309	The system shall provide notification to users when a preliminary print of the U.S. Reports has been superseded by the Bound Volume of U.S. Reports.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-2437	The system shall provide the capability to identify and manage relationships between digital objects, between content packages, and between digital objects and content packages.	Access	Follow Relationships To Other Documents	R2 Must
RD-2438	The system shall provide the capability to identify and manage relationships between digital objects based on changes in content that occur as a result of the legislative process.	Access	Follow Relationships To Other Documents	R2 Must
RD-2439	The system shall provide the capability to identify and manage relationships between digital objects based on changes in content that occur as a result of the regulatory process.	Access	Follow Relationships To Other Documents	R2 Must
RD-3743	The system shall provide the capability to provide bi-directional content relationships.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3823	The system shall provide the capability to access granules in the Weekly Compilation of Presidential Documents based on Weekly Compilation of Presidential Documents citations in the Public Law.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3824	The system shall provide the capability to access House Congressional Bill granules in the Union Calendar Section of the House Calendar based on Union Calendar citations in a House Congressional Bill.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3825	The system shall provide the capability to access Senate Congressional Bill granules in the General Orders Section of the Senate Calendar based on Calendar citations in a Senate Congressional Bill.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3826	The system shall provide the capability to access the U.S. Code based on U.S. Code citations in the Statutes at Large.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3827	The system shall provide the capability to access History of Bill granules in the History of Bills based on bill citations in the Statutes at Large.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3828	The system shall provide the capability to access Congressional Reports based on Congressional Report citations in the Statutes at Large.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3829	The system shall provide the capability to access Congressional Record granules based on Congressional Record citations in the Statutes at Large.	Access	Follow Relationships To Other Documents	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3830	The system shall provide the capability to access the Weekly Compilation of Presidential Documents granules based on Weekly Compilation of Presidential Documents citations in the Statutes at Large.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3831	The system shall provide the capability to access Congressional Reports based on Congressional Report citations in public laws.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3832	The system shall provide the capability to access Statutes at Large granules based Statutes at Large on citations in the U.S. Code.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3833	The system shall provide the capability to access granules the Congressional Directory based on any Members of Congress' name in the Congressional Record.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3834	The system shall provide the capability to access granules in the Congressional Pictorial Directory based on any Members of Congress' name in the Congressional Directory.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3835	The system shall provide the capability to access granules in the Congressional Directory based on any Members of Congress' name in the Congressional Pictorial Directory.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3836	The system shall provide the capability to access granules in the Federal Register based on Regulation Identifier Number in the Unified Agenda.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3837	The system shall provide the capability to access granules in the Federal Register based on Federal Register page number citations in the Unified Agenda.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3838	The system shall provide the capability to access related granules in the Unified Agenda based on Related RIN numbers in the Unified Agenda.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3839	The system shall provide the capability to access an individual Congressional bill granule in the History of Bills based on bill number citation in a Congressional Bill.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3840	The system shall provide the capability to access Congressional Directory granules based on Members of Congress names in the Congressional bills.	Access	Follow Relationships To Other Documents	R1C4 Must
RD-3290	The system shall have the capability to rasterize digital objects.	Access	Format Transformation	R2 Must
RD-3347	The system shall have the capability to convert native files to PDF.	Access	Format Transformation	R1C4 Must
RD-335	The system shall provide the capability to create one or more access derivative renditions for an ACP if its corresponding AIP has no access derivative renditions.	Access	Format Transformation	R1C4 Must
RD-3399	The system shall have the capability to convert images to descriptive ASCII text.	Access	Format Transformation	R1C4 Must
RD-3400	The system shall have the capability to replace images with descriptive text when available while converting digital objects to ASCII.	Access	Format Transformation	R1C4 Must
RD-3402	The system shall have the capability to convert images to descriptive Unicode text.	Access	Format Transformation	R1C4 Must
RD-3403	The system shall have the capability to replace images with descriptive text when available while converting digital objects to Unicode.	Access	Format Transformation	R1C4 Must
RD-3543	The system shall support the transformation of TIFF digital objects into PDF digital objects.	Access	Format Transformation	R1C4 Must
RD-3544	The system shall support the transformation of EPS digital objects into PDF digital objects	Access	Format Transformation	R1C4 Must
RD-3545	The system shall support the transformation of JPG digital objects into PDF digital objects.	Access	Format Transformation	R1C4 Must
RD-3547	The system shall support the transformation of Adobe Photoshop digital objects into PDF digital objects.	Access	Format Transformation	R1C4 Must
RD-3548	The system shall support the transformation of Adobe Illustrator digital objects into PDF digital objects.	Access	Format Transformation	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3549	The system shall support the transformation of Windows Metafile digital objects into PDF digital objects.	Access	Format Transformation	R1C4 Must
RD-3550	The system shall support the transformation of Bitmap digital objects into PDF digital objects.	Access	Format Transformation	R1C4 Must
RD-3551	The system shall support the transformation of locator digital objects into ASCII digital objects.	Access	Format Transformation	R1C4 Must
RD-3552	The system shall support the transformation of SGML digital objects into ASCII digital objects.	Access	Format Transformation	R1C4 Must
RD-533	The system shall have the ability to migrate data to formats other than those in which the files were created or received.	Access	Format Transformation	R2 Must
RD-535	The system shall ensure that the files resulting from migrations will be in a format free of proprietary restrictions to the possible extent.	Access	Format Transformation	R2 Must
RD-536	The system shall have the ability to verify that a file migrated from one format to another retains specified attributes and behaviors, i.e., is authentic and faithful.	Access	Format Transformation	R2 Must
RD-537	The system shall support the transformation of Quark digital objects in previous versions of Quark into Quark digital objects of the current shipping version of Quark as of TBS.	Access	Format Transformation	R2 Must
RD-538	The system shall support the transformation of Quark digital objects into HTML digital objects.	Access	Format Transformation	R1C4 Must
RD-539	The system shall support the transformation of Quark digital objects into ASCII digital objects.	Access	Format Transformation	R1C4 Must
RD-540	The system shall support the transformation of Quark digital objects into XML digital objects.	Access	Format Transformation	R2 Must
RD-541	The system shall support the transformation of Quark digital objects into PDF digital objects.	Access	Format Transformation	R1C4 Must
RD-542	The system shall support the ability to set parameters of the output file of the transformation (resolution, color depth, etc).	Access	Format Transformation	R2 Must
RD-544	The system shall support the transformation of InDesign digital objects in previous versions of InDesign into InDesign digital objects of the current shipping version of InDesign as of TBS.	Access	Format Transformation	R2 Must
RD-545	The system shall support the transformation of InDesign digital objects into HTML digital objects.	Access	Format Transformation	R1C4 Must
RD-546	The system shall support the transformation of InDesign digital objects into ASCII digital objects.	Access	Format Transformation	R1C4 Must
RD-547	The system shall support the transformation of InDesign digital objects into XML digital objects.	Access	Format Transformation	R2 Must
RD-548	The system shall support the transformation of InDesign digital objects into PDF digital objects.	Access	Format Transformation	R1C4 Must
RD-550	The system shall support the transformation of Microsoft Word digital objects in previous versions of Microsoft Word into Microsoft Word digital objects of the current shipping version of Microsoft Word as of TBS.	Access	Format Transformation	R2 Must
RD-551	The system shall support the transformation of Microsoft Word digital objects into HTML digital objects.	Access	Format Transformation	R2 Must
RD-552	The system shall support the transformation of Microsoft Word digital objects into ASCII digital objects.	Access	Format Transformation	R2 Must
RD-553	The system shall support the transformation of Microsoft Word digital objects into XML digital objects.	Access	Format Transformation	R2 Must
RD-554	The system shall support the transformation of Microsoft Word digital objects into PDF digital objects.	Access	Format Transformation	R1C4 Must
RD-555	The system shall support the transformation of Microsoft Word digital objects into Open Document digital objects.	Access	Format Transformation	R2 Must
RD-557	The system shall have the ability to produce notification of incomplete or unsuccessful migrations.	Access	Format Transformation	R2 Must
RD-558	The system shall have the ability to identify incomplete or unsuccessful migrations.	Access	Format Transformation	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-560	The system shall support the transformation of Microsoft Excel digital objects in previous versions of Microsoft Excel into Microsoft Excel digital objects of the current shipping version of Microsoft Excel as of TBS.	Access	Format Transformation	R2 Must
RD-561	The system shall support the transformation of Microsoft Excel digital objects into HTML digital objects.	Access	Format Transformation	R2 Must
RD-562	The system shall support the transformation of Microsoft Excel digital objects into ASCII digital objects.	Access	Format Transformation	R2 Must
RD-563	The system shall support the transformation of Microsoft Excel digital objects into XML digital objects.	Access	Format Transformation	R2 Must
RD-564	The system shall support the transformation of Microsoft Excel digital objects into PDF digital objects.	Access	Format Transformation	R1C4 Must
RD-565	The system shall support the transformation of Microsoft Excel digital objects into Open Document digital objects.	Access	Format Transformation	R2 Must
RD-567	The system shall support the transformation of Microsoft PowerPoint digital objects in previous versions of Microsoft PowerPoint into Microsoft PowerPoint digital objects of the current shipping version of Microsoft PowerPoint as of TBS.	Access	Format Transformation	R2 Must
RD-568	The system shall support the transformation of Microsoft PowerPoint digital objects into HTML digital objects.	Access	Format Transformation	R2 Must
RD-569	The system shall support the transformation of Microsoft PowerPoint digital objects into ASCII digital objects.	Access	Format Transformation	R2 Must
RD-570	The system shall support the transformation of Microsoft PowerPoint digital objects into XML digital objects.	Access	Format Transformation	R2 Must
RD-571	The system shall support the transformation of Microsoft PowerPoint digital objects into PDF digital objects.	Access	Format Transformation	R1C4 Must
RD-572	The system shall support the transformation of Microsoft PowerPoint digital objects into Open Document digital objects.	Access	Format Transformation	R2 Must
RD-574	The system shall support the transformation of PDF digital objects in previous versions of PDF into PDF digital objects of the current shipping version of PDF as of TBS.	Access	Format Transformation	R2 Must
RD-577	The system shall support the transformation of PDF digital objects into XML digital objects.	Access	Format Transformation	R2 Must
RD-578	The system shall support the transformation of HTML digital objects into PDF digital objects.	Access	Format Transformation	R1C4 Must
RD-579	The system shall support the transformation of HTML digital objects into XHTML digital objects.	Access	Format Transformation	R2 Must
RD-581	The system shall support the transformation of HTML digital objects in previous versions of HTML into HTML digital objects of the current version of HTML as of TBS.	Access	Format Transformation	R2 Must
RD-582	The system shall support the transformation of HTML digital objects into ASCII digital objects.	Access	Format Transformation	R2 Must
RD-583	The system shall support the transformation of HTML digital objects into XML digital objects.	Access	Format Transformation	R2 Must
RD-585	The system shall support the transformation of TIFF digital objects in previous versions of TIFF into TIFF digital objects of the current version of TIFF as of TBS.	Access	Format Transformation	R2 Must
RD-586	The system shall support the transformation of the full text index of any TIFF digital object into an ASCII digital object.	Access	Format Transformation	R2 Must
RD-587	The system shall support the transformation of the full text index of any TIFF digital object into an XML digital object.	Access	Format Transformation	R2 Must
RD-588	The system shall support the transformation of the full text index of any TIFF digital object into an HTML digital object.	Access	Format Transformation	R2 Must
RD-589	The system shall support the transformation a TIFF digital object into a JPG digital object.	Access	Format Transformation	R2 Must
RD-590	The system shall support the transformation of the full text index of any TIFF digital object into an PDF digital object.	Access	Format Transformation	R2 Must
RD-592	Where formats containing images are transformed to formats that do not support images (e.g. ASCII, XML) the descriptive text of said images, if any, will be stored in the new format.	Access	Format Transformation	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-593	Where formats containing images are transformed to XML the placement of said images, if any, will be stored in the new format.	Access	Format Transformation	R2 Must
RD-595	The system shall support the transformation of WordPerfect digital objects in previous versions of WordPerfect into WordPerfect digital objects of the current shipping version of WordPerfect as of as of TBS. (RD-595)	Access	Format Transformation	R2 Must
RD-596	The system shall support the transformation of WordPerfect digital objects into Microsoft Word digital objects.	Access	Format Transformation	R2 Must
RD-597	The system shall support the transformation of WordPerfect digital objects into HTML digital objects.	Access	Format Transformation	R2 Must
RD-598	The system shall support the transformation of WordPerfect digital objects into ASCII digital objects.	Access	Format Transformation	R2 Must
RD-599	The system shall support the transformation of WordPerfect digital objects into XML digital objects.	Access	Format Transformation	R2 Must
RD-600	The system shall support the transformation of WordPerfect digital objects into PDF digital objects.	Access	Format Transformation	R2 Must
RD-602	The system shall support the transformation of EPS digital objects in previous versions of EPS into EPS digital objects of the current version of EPS as of as of TBS.	Access	Format Transformation	R2 Must
RD-603	The system shall support the transformation of the full text index of any EPS digital object into an ASCII digital object	Access	Format Transformation	R2 Must
RD-604	The system shall support the transformation of the full text index of any EPS digital object into an XML digital object.	Access	Format Transformation	R2 Must
RD-605	The system shall support the transformation of the full text index of any EPS digital object into an HTML digital object.	Access	Format Transformation	R2 Must
RD-606	The system shall support the transformation of the full text index of any EPS digital object into an PDF digital object.	Access	Format Transformation	R2 Must
RD-607	The system shall support the transformation of JPG digital objects in previous versions of JPG into JPG digital objects of the current version of JPG as of TBS.	Access	Format Transformation	R2 Must
RD-696	The system shall provide the capability to transform text-based granular content into formats that have been optimized for access and delivery if these formats are not already present in the ACP.	Access	Format Transformation	R1C4 Must
RD-3145	The system shall allow authorized users to add information to a knowledge base.	Access	Knowledge Base	R2 Must
RD-3146	The system shall provide the ability for an authorized user to add electronic files to the knowledge base as attachments.	Access	Knowledge Base	R2 Must
RD-3147	The system shall provide the capability to create customized templates for knowledge base entries.	Access	Knowledge Base	R2 Could
RD-3148	The system shall provide the capability for authorized users to choose from a list of templates when creating knowledge base entries.	Access	Knowledge Base	R2 Could
RD-3149	The system shall have the capability to time and date stamp all knowledge base entries.	Access	Knowledge Base	R2 Must
RD-3150	The system shall provide the ability for authorized users to manage information in the knowledge base.	Access	Knowledge Base	R2 Must
RD-3151	The system shall provide the capability to add inquiries and answers from the helpdesk to the knowledge base.	Access	Knowledge Base	R2 Must
RD-3152	The system shall allow authorized users to edit and approve inquiries and responses for addition to the knowledge base.	Access	Knowledge Base	R2 Must
RD-3153	The system shall have the capability for GPO users to recommend helpdesk inquiries and responses for the knowledge base.	Access	Knowledge Base	R2 Must
RD-3154	The system shall provide the ability for authorized users to create categories and subcategories for information stored in the knowledge base.	Access	Knowledge Base	R2 Must
RD-3156	The system shall allow for information stored in the knowledge base to have role-based access restrictions.	Access	Knowledge Base	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3157	The system shall allow for access restrictions to be applied to complete categories.	Access	Knowledge Base	R2 Must
RD-3158	The system shall allow for access restrictions to be applied to individual knowledge base entries.	Access	Knowledge Base	R2 Must
RD-3159	The system shall allow users to assign key words to knowledge base entries.	Access	Knowledge Base	R2 Must
RD-3160	The system shall allow for fields (e.g., subject, title) with an unlimited number of characters.	Access	Knowledge Base	R2 Must
RD-3161	The system shall have the capability for role based access to individual fields on individual knowledge base entries. (e.g., notes field with access to certain GPO employees only)	Access	Knowledge Base	R2 Must
RD-3162	The system shall have the capability for intelligent searching of knowledge base. (e.g., when searching, system asks, “did you mean xxx”?)	Access	Knowledge Base	R2 Must
RD-3163	The system shall provide the capability for users to search the knowledge base by title.	Access	Knowledge Base	R2 Must
RD-3164	The system shall provide the capability for users to search the knowledge base by unique identifiers.	Access	Knowledge Base	R2 Must
RD-3165	The system shall provide the capability to store standard responses for knowledge base entries for use by specific user groups or subgroups.	Access	Knowledge Base	R2 Must
RD-3166	The system shall provide the capability for all users to search the knowledge base.	Access	Knowledge Base	R2 Must
RD-3167	The system shall provide the capability for all users to perform a full-text search the knowledge base.	Access	Knowledge Base	R2 Must
RD-3168	The system shall provide the capability for all users to search the knowledge base by phrase.	Access	Knowledge Base	R2 Must
RD-3169	The system shall provide the capability for all users to search the knowledge base by identification number.	Access	Knowledge Base	R2 Must
RD-3171	The system shall provide the capability to sort knowledge base search results by category.	Access	Knowledge Base	R2 Must
RD-3172	The system shall provide the capability to sort knowledge base search results by subject.	Access	Knowledge Base	R2 Must
RD-3173	The system shall provide the capability to sort knowledge base search results by a default sort.	Access	Knowledge Base	R2 Must
RD-3174	The system shall provide the capability for a user to receive e-mail notification when the content of information stored in a knowledge base entry is updated.	Access	Knowledge Base	R2 Must
RD-3175	The system shall provide the capability to perform records management functions on knowledge base data.	Access	Knowledge Base	R2 Must
RD-3176	The system shall provide the capability to spell-check knowledge base entries before submission.	Access	Knowledge Base	R2 Must
RD-3190	The system shall provide the capability for authorized users to populate the knowledge base with notifications.	Access	Knowledge Base	R2 Must
RD-3854	The system shall ingest all in-scope content on GPO's Federal Bulletin Board	Access	Maintain GPO Access Capabilities	R1C4 Must
RD-3855	The system shall ingest all in-scope content on GPO's Permanent Server.	Access	Maintain GPO Access Capabilities	R1C4 Must
RD-3856	The system shall ingest all in-scope content on GPO Access Web Servers.	Access	Maintain GPO Access Capabilities	R1C4 Must
RD-2585	The system shall provide the capability to maintain PDF features (e.g. bookmarks, comments, links, thumbnails) when individual PDF files are combined into a single PDF file.	Access	Maintain PDF Features	R1C4 Must
RD-2322	The system shall provide the capability to limit access to content with re-dissemination restrictions as specified by authorized users.	Access	Manage Public Access	R1C4 Must
RD-2323	The system shall provide the capability to limit access to content with limited distribution as specified by authorized users.	Access	Manage Public Access	R1C4 Must
RD-2325	The system shall provide the capability to limit access to copyrighted content as specified by authorized users.	Access	Manage Public Access	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2329	The system shall provide the capability to limit access to content based on criteria specified by the Content Originator.	Access	Manage Public Access	R1C4 Must
RD-2330	The system shall provide the capability to limit access to content based on criteria specified by authorized users.	Access	Manage Public Access	R1C4 Must
RD-3732	The system shall provide the capability to prevent an ACP from being created at ingest.	Access	Manage Public Access	R1C4 Must
RD-2312	The system shall provide the capability to provide access to select external repositories with which GPO has formal partnership agreements including Census 200 data (U.S. Census Bureau/Case Western Reserve University): Established a Web site specifically for depository library access to Census 2000 data issued by the Census Bureau in comma-delimited ASCII format.	Access	Partnerships	R1C4 Must
RD-2313	The system shall provide the capability to provide access to select external repositories with which GPO has formal partnership agreements including a partnership between GPO and the Indiana University, Bloomington Libraries on behalf of the Committee on Institutional Cooperation, making publications that were distributed to Federal Depository Libraries on floppy disk available over the Internet.	Access	Partnerships	R1C4 Must
RD-2314	The system shall provide the capability to provide access to select external repositories with which GPO has formal partnership agreements including CyberCemetery (University of North Texas): Provide permanent online access to electronic publications of selected federal Government agencies which have ceased operation.	Access	Partnerships	R1C4 Must
RD-2315	The system shall provide the capability to provide access to select external repositories with which GPO has formal partnership agreements including FRASER (Federal Reserve Bank of St. Louis): Provides for public access to content in the Federal Reserve Archival System for Economic Research (FRASER) service.	Access	Partnerships	R1C4 Must
RD-2316	The system shall provide the capability to provide access to select external repositories with which GPO has formal partnership agreements including National Library of Medicine: Provides permanent public access to Medline, Medical Subject Headings, and NLM LocatorPlus.	Access	Partnerships	R1C4 Must
RD-2317	The system shall provide the capability to provide access to select external repositories with which GPO has formal partnership agreements including National Renewable Energy Laboratory: Provides permanent public access to NREL's laboratory and outreach publications.	Access	Partnerships	R1C4 Must
RD-2318	The system shall provide the capability to provide access to additional select external repositories with which GPO has formal partnership agreements.	Access	Partnerships	R2 Must
RD-2562	The system shall provide the capability to search cataloging records in order to provide access to select external repositories with which GPO has formal partnership agreements as specified in requirements RD-2312 throughRD-2318 and RD-3555 through RD-3556.	Access	Partnerships	R2 Must
RD-3555	The system shall provide the capability to provide access to select external repositories with which GPO has formal partnership agreements including Historic Government Publications from World War II: A partnership between GPO and the Central University Libraries of Southern Methodist University that provides permanent public access to digitized copies of U.S. Government publications distributed by GPO during World War II.	Access	Partnerships	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3556	The system shall provide the capability to provide access to select external repositories with which GPO has formal partnership agreements including Historic Publications of the United States Commission on Civil Rights: A partnership between GPO, the Thurgood Marshall Law Library, the University of Maryland School of Law, and the U.S. Commission on Civil Rights that provides permanent public access to historical and current publications of the U.S. Commission on Civil Rights from the Thurgood Marshall Law Library Web site.	Access	Partnerships	R1C4 Must
RD-2909	The system shall have the ability to generate lists based on any metadata field.	Access	Reference Tools	R2 Must
RD-2910	The system shall have the capability to generate lists based on search query (e.g., that match a library's item selection profile).	Access	Reference Tools	R2 Must
RD-2911	The system should have the capability to generate lists that point to content (e.g., electronic journals, lists of products that are available for purchase from the GPO Sales Program).	Access	Reference Tools	R2 Must
RD-2912	The system should have the capability to generate lists that point to metadata (e.g., lists of publications available for selection by depository libraries).	Access	Reference Tools	R2 Must
RD-2913	The system should have the capability to generate lists that point to related resources or other reference tools (e.g., Browse Topics).	Access	Reference Tools	R2 Should
RD-2914	The system shall have the capability to link to external content and metadata.	Access	Reference Tools	R2 Must
RD-2915	The system shall be interoperable with third party reference tools (e.g., search catalogs of other libraries).	Access	Reference Tools	R3 Should
RD-2916	The system shall have the capability to dynamically generate reference tools.	Access	Reference Tools	R3 Could
RD-2917	The system will allow GPO to manage reference tools.	Access	Reference Tools	R2 Must
RD-2918	The system will allow GPO to add reference tools.	Access	Reference Tools	R2 Must
RD-2919	The system will allow GPO to update reference tools with capability of saving previous versions	Access	Reference Tools	R2 Must
RD-2920	The system will allow GPO to delete reference tools, with capability of saving previous versions.	Access	Reference Tools	R2 Must
RD-2921	The system shall be able to generate lists based on user preferences.	Access	Reference Tools	R2 Must
RD-2922	The system shall provide the capability for users to customize reference tools.	Access	Reference Tools	R2 Must
RD-2744	The system shall allow users with an established user account and profile to enter or store queries, preferences, and results sets or portions of results sets.	Access	Save Search Query	R2 Must
RD-2745	The system shall allow users with an established user account and profile to enter or store and recall queries.	Access	Save Search Query	R2 Must
RD-2746	The system shall allow users with an established user account and profile to enter or store and recall preferences.	Access	Save Search Query	R2 Must
RD-2749	The system shall provide the capability to automatically execute saved searches on a schedule defined by the user.	Access	Save Search Query	R2 Must
RD-2750	The system shall provide the capability to notify users when automatically executed searches return results that were not included in the original search.	Access	Save Search Query	R2 Must
RD-2737	The system shall allow users to save search results individually or as a batch (e.g., without selecting each result individually) for delivery.	Access	Save Search Results	R1C4 Must
RD-2747	The system shall allow users with an established user account and profile to enter or store and recall results sets as a whole.	Access	Save Search Results	R2 Must
RD-2748	The system shall allow users with an established user account and profile to enter or store and recall portions of results sets.	Access	Save Search Results	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2590	The system shall provide the capability to apply business rules to user queries so that content is searched based on query (e.g., intelligent search).	Access	Search	R2 Must
RD-2641	The system shall provide access to the eCFR (Electronic Code of Federal Regulations) collection.	Access	Search	R1C4 Must
RD-2672	The system shall allow users to perform a search for conceptually related terms (e.g., search for "World Series" returns articles on the Red Sox).	Access	Search	R1C4 Must
RD-2673	The system shall allow authorized users to manage concept relationships.	Access	Search	R1C4 Must
RD-2674	The system shall allow authorized users to add concept relationships.	Access	Search	R1C4 Must
RD-2675	The system shall allow authorized users to delete concept relationships.	Access	Search	R1C4 Must
RD-2676	The system shall allow authorized users to modify concept relationships.	Access	Search	R1C4 Must
RD-2677	The system shall suggest new concept relationships based on ingested content.	Access	Search	R1C4 Must
RD-2678	The system shall automatically create new concept relationships based on an authorized users acceptance of suggested new concept relationships	Access	Search	R1C4 Must
RD-2679	The system shall use new concepts without requiring previously indexed content be re-indexed.	Access	Search	R1C4 Must
RD-2687	The system shall allow users to perform a natural language search.	Access	Search	R1C4 Must
RD-2691	The system shall allow for left side stemming.	Access	Search	R1C4 Should
RD-2709	The system shall provide the capability to display a list of terms that are conceptually related to the original search term.	Access	Search	R1C4 Must
RD-2710	The system shall provide users with the ability to directly execute a search from conceptually related terms.	Access	Search	R1C4 Must
RD-2724	The system shall provide the capability to apply one or multiple taxonomies.	Access	Search	R1C4 Must
RD-2761	The system shall provide for the control of search run times, including the ability to preempt runtimes by an administrator-defined limit.	Access	Search	R2 Must
RD-3759	The system shall provide the capability for users to search by all fields in schema registered with the system.	Access	Search	R2 Must
RD-3760	The system shall allow users to search inside publications.	Access	Search	R1C4 Must
RD-2699	The system shall have a documented interface (e.g., API) to allow search by non-GPO systems.	Access	Search Interface for External Systems	R1C4 Must
RD-2412	The system shall have the capability to provide recommendations for content and services based on preferences and queries of users and groups of similar users.	Access	Search Results	R2 Must
RD-2714	The system shall have the capability to take users to the exact occurrence of the search term or its conceptual equivalent in a result.	Access	Search Results	R1C4 Must
RD-2720	The system shall provide the capability to categorize results.	Access	Search Results	R1C4 Must
RD-2721	The system shall provide the capability to cluster results.	Access	Search Results	R1C4 Must
RD-2722	The system shall provide the capability to analyze results.	Access	Search Results	R2 Could
RD-2723	The system shall provide the capability to display results graphically.	Access	Search Results	R2 Could
RD-2728	The system shall allow a result set equal to the size of all records in all indexes.	Access	Search Results	R2 Must
RD-2733	The system shall provide the capability to highlight query terms in the document.	Access	Search Results	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2734	The system shall provide the capability to highlight query terms in the document abstract or document summary that appears results list.	Access	Search Results	R2 Must
RD-2736	The system shall provide the capability to display inline image thumbnails of content in a results list.	Access	Search Results	R2 Must
RD-2739	The system shall provide the capability for authorized users to modify relevancy ranking factors.	Access	Search Results	R1C4 Must
RD-3772	The system shall provide the capability to group versions into one entry in a search results list.	Access	Search Results	R1C4 Must
RD-3774	The system shall provide the capability for users to hide document summaries so they do not display in search results.	Access	Search Results	R1C4 Must
RD-3742	The system shall provide the capability for users to access select agency publications at a level of granularity that is less than a publication.	Access	Support Granularity	R2 Must
RD-3786	The system shall record content relationships in metadata.	Access	Support Granularity	R1C2 Must
RD-648	The system shall provide the capability to create new granules by aggregating and decomposing existing granules.	Access	Support Granularity	R2 Must
RD-667	The system shall support granularity down to the level of any paragraph in a publication.	Access	Support Granularity	R1C4 Should / R2 Must
RD-668	The system shall support granularity down to the level of any individual graphic.	Access	Support Granularity	R1C4 Must
RD-669	The system shall support granularity down to the level of any embedded graphical element in a publication.	Access	Support Granularity	R1C4 Should / R2 Must
RD-671	The system shall support granularity down to the level of any frame of a video.	Access	Support Granularity	R3 Must
RD-673	The system shall support granularity of audio down to smallest segment of time the audios encoding allows.	Access	Support Granularity	R3 Should
RD-3193	The system shall provide users access to training materials and training history.	Access	Training and Events	R2 Could
RD-3194	The system shall provide access to training materials available as digital video.	Access	Training and Events	R2 Could
RD-3195	The system shall provide access to training materials available as digital documents.	Access	Training and Events	R2 Could
RD-3196	The system shall provide access to training materials available as digital audio.	Access	Training and Events	R2 Could
RD-3197	The system shall provide access to training materials available as digital multimedia.	Access	Training and Events	R2 Could
RD-3198	The system shall provide access to training materials available in other formats.	Access	Training and Events	R2 Could
RD-3199	The system shall allow authorized users to manage training materials and training history.	Access	Training and Events	R2 Could
RD-3200	The system shall have the capability for authorized users to restrict access to training material and training history.	Access	Training and Events	R2 Could
RD-3201	The system shall provide the capability to restrict access to training materials based on user role.	Access	Training and Events	R2 Could
RD-3202	The system shall provide the capability to restrict access to training materials based on user group.	Access	Training and Events	R2 Could
RD-3203	The system shall allow users to enroll in training and events.	Access	Training and Events	R2 Could
RD-3204	The system shall allow authorized users to manage training and events.	Access	Training and Events	R2 Could
RD-3205	The system shall provide interactive training.	Access	Training and Events	R2 Could
RD-3206	The system shall provide interactive self-paced training.	Access	Training and Events	R2 Could
RD-3207	The system shall provide interactive instructor-led training.	Access	Training and Events	R2 Could
RD-3208	The system shall provide users verification of enrollment in training and events.	Access	Training and Events	R2 Could

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3209	The system shall provide the capability for users to measure their progress and performance in training.	Access	Training and Events	R2 Could
RD-3210	The system shall provide the capability for users to provide feedback on training.	Access	Training and Events	R2 Could
RD-3211	The system shall provide online tutorials.	Access	Training and Events	R2 Could
RD-3048	The system shall provide phone numbers for users to contact authorized users for user assistance based on their user profile and the function they are performing.	Access	User Help	R2 Could
RD-3049	The system shall provide e-mail addresses for users to contact authorized users for user assistance based on their user profile and the function they are performing.	Access	User Help	R2 Must
RD-3050	The system shall provide mailing addresses for users to contact authorized users for user assistance based on their user profile and the function they are performing.	Access	User Help	R2 Could
RD-3051	The system shall provide real-time text chat for users to contact GPO Service Specialists for user assistance.	Access	User Help	R2 Could
RD-3052	The system shall provide Facsimile numbers for users to contact authorized users for user assistance based on their user profile and the function they are performing.	Access	User Help	R2 Could
RD-3056	The system shall provide phone numbers for authorized users to contact users for user assistance.	Access	User Help	R2 Could
RD-3057	The system shall provide e-mail addresses for GPO Service Specialists to contact users for user assistance.	Access	User Help	R2 Must
RD-3058	The system shall provide real-time text chat for authorized users to contact users for user assistance.	Access	User Help	R2 Could
RD-3059	The system shall provide facsimile numbers for authorized users to contact users for user assistance.	Access	User Help	R2 Could
RD-3061	The system shall provide users with the ability to opt-out of user support features.	Access	User Help	R1C4 Must
RD-3062	The system shall provide users with the ability to enable or disable context specific help that consists of customizable descriptive text displayed when a user points the mouse over an item on the user interface.	Access	User Help	R1C4 Must
RD-3063	The system shall provide users with the ability to enable or disable context specific help that consists of clickable help icons or text on the user interface.	Access	User Help	R1C4 Must
RD-3064	The system shall have the capability to provide for address hygiene utilizing CASS certified and National Change of Address certified software to minimize delivery risks.	Access	User Help	R2 Could
RD-3065	The system shall have the capability for Computer Telephone Integration (CTI) with auto screen pop-ups to integrate the agency's telephone and order management systems.	Access	User Help	R2 Could
RD-3066	The system shall have the capability to integrate with GPO's Automated Call Dialer (ACD) system to allow for automatic consumer telephone access to account and transaction data.	Access	User Help	R2 Could
RD-3067	The system shall have the capability to process e-mail marketing campaigns	Access	User Help	R2 Could
RD-3070	Content of context specific help shall be related to what is being viewed on the screen and shall be dynamically generated.	Access	User Help	R2 Could / R3 Must
RD-3084	The system shall provide the capability for authorized users to manage information that is displayed as a result of clicking on a help icon or text.	Access	User Help	R2 Must
RD-3088	The system shall have the capability to support a helpdesk to route, track, prioritize, and resolve user inquiries to authorized users.	Access	User Helpdesk	R2 Must
RD-3092	The system shall have the capability to receive helpdesk inquiries from registered and non-registered users.	Access	User Helpdesk	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3093	The system shall have the capability to maintain user identification for helpdesk inquiries and responses after a user no longer has a registered account in the system.	Access	User Helpdesk	R2 Must
RD-3094	The system shall provide the capability for users to select from lists of categories when submitting inquiries to the helpdesk.	Access	User Helpdesk	R2 Must
RD-3095	The system shall provide the capability for users to select from subgroups of categories when submitting inquiries to the helpdesk.	Access	User Helpdesk	R2 Must
RD-3096	The system shall provide the capability for authorized users to manage categories and subcategories of inquiries that are submitted to the helpdesk.	Access	User Helpdesk	R2 Must
RD-3097	The system shall provide the capability for a user to attach files when submitting inquiries to the helpdesk.	Access	User Helpdesk	R2 Must
RD-3098	The system shall have the capability to notify users that their inquiry has been received by the helpdesk	Access	User Helpdesk	R2 Must
RD-3099	The system shall provide the capability to record the time and date of all inquiries and responses that sent and received by the helpdesk.	Access	User Helpdesk	R2 Must
RD-3100	The system shall provide the capability to notify an authorized user that they have been assigned an inquiry by the helpdesk.	Access	User Helpdesk	R2 Must
RD-3101	The system shall have the capability to route, track, and prioritize helpdesk inquiries and responses received.	Access	User Helpdesk	R2 Must
RD-3102	The helpdesk shall have the capability to support multiple departments and additional future departments, when needed.	Access	User Helpdesk	R2 Must
RD-3103	The helpdesk and knowledge base shall have the capability to synchronize with data entered into the system while not connected to the internet.	Access	User Helpdesk	R2 Must
RD-3104	The helpdesk shall have the capability to integrate with user account information and additional sources of business process information stored outside of the helpdesk. (e.g., Oracle, user accounts in Storage/Access)	Access	User Helpdesk	R2 Must
RD-3105	Other systems/functional elements shall have the capability to access information stored in the helpdesk.	Access	User Helpdesk	R2 Must
RD-3106	The helpdesk shall have the capability to access information stored in other systems/functional elements.	Access	User Helpdesk	R2 Must
RD-3107	The system shall allow users to specify job numbers (e.g., CO Ordering numbers, Request Ordering numbers) and other identifiers (e.g., voucher numbers, ISBN numbers) in helpdesk inquiry fields.	Access	User Helpdesk	R2 Must
RD-3108	The system shall allow users to select from various templates for submission of inquiries to the helpdesk. (e.g., complaint template for CO Order, template for phone conversation, template for contract modification request)	Access	User Helpdesk	R2 Must
RD-3109	The system shall assign unique identifiers based on the type of helpdesk template used. (e.g., to track complaints, modification requests)	Access	User Helpdesk	R2 Must
RD-3110	The system shall allow authorized GPO users to manage templates for submission of helpdesk inquiries.	Access	User Helpdesk	R2 Must
RD-3111	The system shall have the capability for role based access to individual fields on individual helpdesk inquiries and responses. (e.g., Notes field with access to GPO employees only)	Access	User Helpdesk	R2 Must
RD-3112	The system shall have the capability to display all helpdesk inquiries and responses related to a particular job number (e.g., Request order number, CO Order number) or other unique identifier. (e.g., voucher numbers, ISBN numbers)	Access	User Helpdesk	R2 Must
RD-3113	The system shall allow authorized users to manually create a new helpdesk inquiry in order to accommodate inquiries that do not enter the system electronically.	Access	User Helpdesk	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3114	The system shall provide the capability to queue inquiries submitted to the helpdesk.	Access	User Helpdesk	R2 Must
RD-3115	The system shall support priority processing of inquiries submitted to the helpdesk.	Access	User Helpdesk	R2 Must
RD-3116	The system shall provide the capability for authorized users to manage the status categories for inquires submitted to the helpdesk.	Access	User Helpdesk	R2 Must
RD-3117	The system shall provide the capability for authorized users to restrict access to helpdesk inquiry tracking.	Access	User Helpdesk	R2 Must
RD-3118	The system shall provide automated routing of helpdesk inquiries to the departments/individuals based on workflow.	Access	User Helpdesk	R2 Must
RD-3119	The system shall provide automated routing of helpdesk inquiries to the departments/individuals based on selections made by the user when an inquiry is made.	Access	User Helpdesk	R2 Must
RD-3120	The system shall provide automated routing of helpdesk inquiries to the departments/individuals based on keywords in the inquiry sent by the user.	Access	User Helpdesk	R2 Must
RD-3121	The system shall provide automated routing of helpdesk inquiries to the departments/individuals based on the user role and group of the inquirer.	Access	User Helpdesk	R2 Must
RD-3124	The system shall provide the capability for authorized users to route helpdesk inquiries to individuals	Access	User Helpdesk	R2 Must
RD-3125	The system shall provide the capability for authorized users to route helpdesk inquiries to departments.	Access	User Helpdesk	R2 Must
RD-3126	The system shall provide the capability for authorized users route helpdesk inquiries to users via an email notification.	Access	User Helpdesk	R2 Must
RD-3127	The system shall provide the capability for authorized users to specify the departments or individuals.	Access	User Helpdesk	R2 Must
RD-3128	The system shall provide the capability for users to determine the departments they wish to request an answer from.	Access	User Helpdesk	R2 Must
RD-3129	The system shall provide the capability for users to determine the individuals they wish to request a helpdesk answer from.	Access	User Helpdesk	R2 Must
RD-3130	The system shall provide the capability to request user feedback regarding quality of a response given by the helpdesk.	Access	User Helpdesk	R2 Must
RD-3131	The system shall provide users with access to history of their inquiries and responses submitted to and received from the helpdesk.	Access	User Helpdesk	R2 Must
RD-3132	The system shall store helpdesk inquiries and responses.	Access	User Helpdesk	R2 Must
RD-3133	The system shall have the capability to allow authorized users to amend inquiries and responses submitted to and received from the helpdesk.	Access	User Helpdesk	R2 Must
RD-3134	The system shall provide the capability for users to search helpdesk inquiries and responses.	Access	User Helpdesk	R2 Must
RD-3135	The system shall provide the capability for authorized users to search for helpdesk inquiries by any defined field.	Access	User Helpdesk	R2 Must
RD-3136	The system shall support the capability to monitor the quality of responses given by helpdesk staff.	Access	User Helpdesk	R2 Must
RD-3137	The system shall provide the capability to provide users with access to helpdesk inquiries from other users related to their queries.	Access	User Helpdesk	R2 Must
RD-3138	The system shall provide the capability for users to search helpdesk inquiries from other users.	Access	User Helpdesk	R2 Must
RD-3139	The system shall provide the capability to assign user access rights to individual helpdesk inquiries and responses.	Access	User Helpdesk	R2 Must
RD-3140	The system shall provide the capability to record users responding to helpdesk inquiries.	Access	User Helpdesk	R2 Must
RD-3141	The system shall provide the capability to log helpdesk information exchanges.	Access	User Helpdesk	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3142	The system shall provide the capability to store metadata related to what is being discussed via the helpdesk.	Access	User Helpdesk	R2 Must
RD-3143	The system shall provide the capability for users to spell-check inquiries and responses before submitting them to the helpdesk.	Access	User Helpdesk	R2 Must
RD-3155	The system shall provide the capability to store standard helpdesk responses for use by specific user groups or subgroups.	Access	User Helpdesk	R2 Must
RD-2402	Preferred contact methods	Access	User Interface	R2 Must
RD-2403	Delivery options	Access	User Interface	R2 Must
RD-2405	Alert services	Access	User Interface	R2 Must
RD-2406	Help features	Access	User Interface	R2 Must
RD-2407	Frequently accessed tools	Access	User Interface	R2 Must
RD-2408	Search preferences	Access	User Interface	R2 Must
RD-2409	The system shall provide the capability for authorized users to manage future user preferences.	Access	User Interface	R2 Must
RD-2754	The system shall provide the capability to have customizable search interfaces based on user preferences.	Access	User Interface	R2 Must
RD-2972	The system shall provide for non-English language extensibility such that GUIs could contain non-English language text.	Access	User Interface	R2 Must
RD-2998	GUIs shall be developed in accordance with the Research Based Web Design & Usability Guidelines, 2006 edition.	Access	User Interface	R1C4 Must
RD-2999	Web GUIs shall be developed in accordance with the Web Style Guide, 2nd edition.	Access	User Interface	R1C4 Must
RD-3011	The system shall conform to WML.	Access	User Interface	R2 Must
RD-3014	The system shall provide the capability for users to customize GUIs by adding tools.	Access	User Interface	R2 Must
RD-3015	The system shall provide the capability for users to customize GUIs by removing tools.	Access	User Interface	R2 Must
RD-3016	The system shall provide the capability for users to customize GUIs by hiding tools.	Access	User Interface	R2 Must
RD-3017	The system shall provide the capability for users to customize GUIs by changing the placement of tools.	Access	User Interface	R2 Must
RD-3018	The system shall provide the capability for users to customize GUIs by modifying the size of tools.	Access	User Interface	R2 Must
RD-3019	The system shall provide the capability for users to customize GUIs by selecting text size from available options.	Access	User Interface	R2 Must
RD-3020	The system shall provide the capability for users to customize GUIs by selecting color scheme from available options.	Access	User Interface	R2 Must
RD-3023	The system shall provide the capability for users to revert to default GUIs as displayed prior to any customization.	Access	User Interface	R2 Must
RD-3024	The system shall provide the capability for users to maintain GUI configurations across user sessions.	Access	User Interface	R2 Must
RD-3032	The system must provide a GUI for GPO Business Managers that is based on their user role.	Access	User Interface	R2 Must
RD-3810	The system shall provide a public user GUI that allows users to select files to be packaged as a DIP.	Access	User Interface	R1C4 Must
RD-3814	The system shall provide a public user GUI that allows users to access publications on partner web sites.	Access	User Interface	R1C4 Must
RD-3815	The system shall provide a public user GUI that allows users to sign up to receive an email notification when new publications are available that match their search query.	Access	User Interface	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3816	The system shall provide a public user GUI that allows users to sign up to receive an email notification when new publications are added to GPO defined collections.	Access	User Interface	R1C4 Must
RD-3847	The system shall provide the capability for authorized users to manually create new Web pages.	Access	User Interface	R1C4 Must
RD-3848	The system shall provide the capability to display public user GUIs on mobile devices.	Access	User Interface	R2 Must
RD-2828	The system shall provide the capability to notify End Users when their subscriptions are about to end (e.g., renewal notices).	Access	User Notification	R2 Must
RD-2829	The system shall provide the capability to deliver personalized offers based on individual user request history or users with similar request histories. (e.g. "you may also be interested in…").	Access	User Notification	R2 Must
RD-2830	The system shall provide the capability for users to opt-out of personalized offers.	Access	User Notification	R2 Must
RD-3179	The system shall allow all users to subscribe and unsubscribe to notification services	Access	User Notification	R1C4 Must
RD-3181	The system shall provide email notifications.	Access	User Notification	R1C4 Must
RD-3182	The system shall provide RSS notifications that conform to the RSS 2.0 specification.	Access	User Notification	R1C4 Must
RD-3184	The system shall allow users to choose notification delivery method from a list of available options.	Access	User Notification	R1C4 Must
RD-3185	The system shall provide the capability to provide notifications based on user profiles and history.	Access	User Notification	R2 Must
RD-3186	The system shall have the capability to automatically send notifications to users based on system events.	Access	User Notification	R1C4 Must
RD-3187	The system shall have the capability to automatically send notifications based on business events (e.g., new version of publication available, new services available).	Access	User Notification	R1C4 Must
RD-3188	The system shall have the capability to automatically send notifications to authorized users based on job processing events.	Access	User Notification	R1C4 Must
RD-3189	The system shall provide the capability for authorized users to create new notification categories for manually generated notifications.	Access	User Notification	R1C4 Must
RD-3272	The system shall have the capability to provide notification of delivery fulfillment based on user preferences.	Access	User Notification	R2 Must
RD-3273	The system shall have the capability to provide notification of delivery fulfillment based on information gathered at time of request.	Access	User Notification	R2 Must
RD-3718	The system shall provide the capability for public users to receive an email notification when new publications are added to a collection.	Access	User Notification	R1C4 Must
RD-3719	The system shall provide the capability for public users to receive an email notification when new publications are added to the system.	Access	User Notification	R1C4 Must
RD-3720	The system shall provide the capability for public users to receive an RSS notification when new publications are added to a collection.	Access	User Notification	R1C4 Must
RD-3721	The system shall provide the capability for public users to receive an RSS notification when new publications are added to the system.	Access	User Notification	R1C4 Must
RD-3818	The system shall provide the capability to send a notification to users when there is a new match to a user defined string.	Access	User Notification	R1C4 Must

3.2 BULK SIGNING FEATURE GROUP REQUIREMENTS

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3863	The system shall provide the capability to validate digitally signed documents in bulk.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3864	The integrity mark shall provide the capability to include the GPO Seal of Authenticity logo when the digital signature is a visible digital signature	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3865	The integrity mark shall provide the capability to include other Federal Government logos when the digital signature is a visible digital signature.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3866	The system shall provide the capability to customize the display of all signature properties when the digital signature is a visible digital signature.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3867	The system shall provide the capability to certify a new signature field.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3868	The system shall provide the capability to certify an existing signature field.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3869	The system shall provide the capability to sign a new signature field.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3870	The system shall provide the capability to sign an existing signature field.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3871	The system shall provide the capability to validate existing signature fields automatically without user intervention to input the name of the existing signature fields.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3872	The system shall provide the capability for authorized users to clear an existing signature field that contains a signing signature.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3873	The system shall provide the capability for authorized users to clear an existing signature field that contains a certifying signature.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3874	The system shall provide the capability to record in metadata the signature field names used in signing in the signing process.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3875	The system shall provide the capability to record in metadata the signature field names used in the certifying process.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3876	The system shall provide the capability to record in metadata the signature field names used in the validation process.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3877	The system shall provide the capability to validate a digitally signed document without changing the file name of that document as part of the validation process.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3878	The system shall provide the capability to specify the height of an integrity mark when it is applied to a set number of documents.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3879	The system shall provide the capability to specify the width of an integrity mark when it is applied to a set number of documents.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3880	The system shall provide the capability to specify the page number for the application of an integrity mark to a set number of documents.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3881	The system shall provide the capability to add an integrity mark to one page of a document.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-3882	The system shall provide the capability to add an integrity mark to multiple pages of a document.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-769	The system shall provide the capability to certify content as authentic.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-776	The system shall provide the capability to certify content as official.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-778	The system shall provide the capability to certify content at levels of granularity defined by GPO.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-779	The system shall provide the capability to convey certification by means of an integrity mark.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-780	The system shall provide the capability to use GPO's Public Key Infrastructure (PKI).	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-783	The system shall provide the capability to use public key cryptography, digital certificates, encryption or other widely accepted information security mechanisms for providing authentication services within FDsys.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-785	The system shall provide the capability to verify and validate the authenticity, integrity, and official status of deposited content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-801	The system shall have the capability to use PKI for the establishment of a trust model for deposited content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-803	The system shall provide the capability to validate the authenticity of harvested content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-804	The system shall provide the capability to validate the integrity of harvested content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-805	The system shall provide the capability to validate the official status of harvested content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-827	The system shall have the capability to use PKI for the establishment of a trust model for converted content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-831	The system shall have the capability to retain integrity marks in accordance with GPO business rules.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-872	The system shall have the capability to certify integrity of delivered content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-873	The system shall have the capability to apply a cryptographic digital signature, in accordance with IETF RFC 3447, to content delivered from the system.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-890	The system shall provide the capability of demonstrating continued integrity of content packages when authorized changes are made (such as to the metadata).	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-899	The system shall support the use of integrity marks.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-900	Integrity marks shall include certification information.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-901	Integrity marks shall employ widely accepted information security mechanisms (e.g., public key cryptography, digital certificates, digital signatures, XML signatures, digital watermarks, or traditional watermarks).	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-902	The system shall support the capability to manually add integrity marks to content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Could
RD-903	The system shall support the capability to automatically add integrity marks to content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-904	The system shall support the use of visible integrity marks.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-905	The system shall support the use of invisible integrity marks.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-907	The system shall provide flexibility regarding where the integrity mark is applied through automated processes.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-908	The system shall provide flexibility regarding where the integrity mark is applied through manual processes.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-909	The system shall provide the capability to automatically position the exact location (x, y coordinates) of where an integrity mark is applied for any set number of documents.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-910	The system shall support the application of multiple integrity marks on the same content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-911	The system shall support the application of security policies, such that integrity marks can be applied to content in particular sequences depending on levels of authority.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-914	The system shall provide the capability for users to validate the authenticity of the content packages that are delivered from the system.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-915	The system shall provide the capability for users to validate the integrity of the content packages that are delivered from the system.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-916	The system shall provide the capability for users to validate the official status of the content packages that are delivered from the system.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-918	The system shall enable GPO to add integrity marks to FDsys content that is delivered to End Users in the form of electronic presentation.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-919	The system shall enable GPO to add integrity marks to FDsys content that is delivered to End Users in the form of hard copy output.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-920	The system shall enable GPO to add integrity marks to FDsys content that is delivered to End Users in the form of digital media.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-923	Where public key cryptography and digital certificates are used to create a digital signature integrity mark on delivered content the following shall apply:	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-924	The integrity mark shall provide the capability to include the GPO Seal of Authenticity logo if the digital signature is a visible digital signature.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Could
RD-925	The integrity mark shall include certification information.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-926	The integrity mark shall include the name of the certifying organization.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-927	The integrity mark shall include the date on the signer's digital certificate.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-928	The integrity mark shall include the digital time stamp.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-929	The integrity mark shall include the public key value of the signer.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-930	The integrity mark shall include identification of the hash algorithm used.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-931	The integrity mark shall include the reason for signing.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-932	The integrity mark shall include the signer's location.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-933	The integrity mark shall include the signer's contact information.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-934	The integrity mark shall include the name of the entity that certified the content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-935	The integrity mark shall include the expiration date of the digital certificate used to sign the content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-936	The integrity mark shall be flexible enough to include additional, GPO-defined certification information.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-937	The values for the integrity mark fields shall be extracted from the digital certificate that was used to create the digital signature.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-940	The system shall have the capability to confirm that the digital certificate that was used to create the digital signature is valid and accurate.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-941	As a result of the digital signature validation check, the system should notify users if the digital certificate is valid, invalid, or cannot be validated.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-942	The system shall have the capability to perform a bit for bit comparison of the digital object as it was at the time of signing against the document as it was at the time of the validation check. As a result of the validation check, the system should notify users if the content has been modified, has not been modified, or if the system cannot determine if the content has been modified.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-943	The system shall have the capability to perform a bit for bit comparison of the digital object as it was at the time of signing against the document as it was at the time of the validation check.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-944	As a result of the validation check, the system should notify users if the content has been modified, has not been modified, or if the system cannot determine if the content has been modified.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-946	The digital signature shall include the date and time that the digital signature was applied to content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-947	The digital signature shall include the expiration date of the digital certificate.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-950	For digitally signed PDFs delivered to end users, the validity of the digital certificate shall be based on the certificate validity at the time and date the content was digitally signed.	Bulk Signing	PDF Signing Using Bulk Signing System	R1C3 Should / R2 Must
RD-951	For electronic presentation, validation shall be done automatically without End User intervention.	Bulk Signing	PDF Signing Using Bulk Signing System	R1C3 Should / R2 Must
RD-953	The system shall provide the capability to re-authenticate content that has already been authenticated (e.g., expired certificate).	Bulk Signing	PDF Signing Using Bulk Signing System	R1C3 Should / R2 Must
RD-954	The system shall provide the capability to notify GPO System Administrators when content needs to be re-authenticated.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-955	The system shall provide the capability for GPO to change or revoke the authentication status of content.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-979	The system shall create administrative records of authentication processes.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-981	The system shall support an audit capability for content certification.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-982	The system shall support an audit capability for content validation.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-983	The system shall comply with GPO and Federal records management policies.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-984	The system shall comply with GPO records management policies, as document in GPO Publication 840.7.	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must
RD-985	The system shall comply with Federal records management policies (e.g., NARA's Records Management Guidance for Agencies Implementing Electronic Signature Technologies, 2000).	Bulk Signing	PDF Signing Using Bulk Signing System	R2 Must

3.3 CONGRESSIONAL SUBMISSION FEATURE GROUP REQUIREMENTS

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2964	Content Originator GUIs shall be section 508 compliant.	Congressional Submission	508 Compliant User Interfaces	R1C3 Must
RD-2967	The system shall maintain a consistent look and feel throughout authorized user GUIs.	Congressional Submission	508 Compliant User Interfaces	R1C2 Must
RD-3697	Service Provider GUIs shall be section 508 compliant according to 36 CFR Part 1194.21.	Congressional Submission	508 Compliant User Interfaces	R1C2 Must
RD-3698	Service Specialist GUIs shall be section 508 compliant according to 36 CFR Part 1194.21.	Congressional Submission	508 Compliant User Interfaces	R1C2 Must
RD-1866	The system shall allow users to search job BPI related to a user account or agency.	Congressional Submission	Authorized User Search	R1C3 Must
RD-2068	The system shall allow users to search job BPI.	Congressional Submission	Authorized User Search	R1C3 Must
RD-2368	The system shall provide the capability for authorized users to access WIP storage.	Congressional Submission	Authorized User Search	R1C3 Must
RD-2369	The system shall have the capability to allow authorized users to authorize access to content in WIP.	Congressional Submission	Authorized User Search	R1C3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2559	The system shall provide the capability to search across multiple internal content and metadata collections simultaneously.	Congressional Submission	Authorized User Search	R1C2 Must
RD-2560	The system shall provide the capability to search content and metadata collections separately.	Congressional Submission	Authorized User Search	R1C2 Must
RD-2569	The system shall provide the capability for authorized users to search collections constrained by user role.	Congressional Submission	Authorized User Search	R1C2 Must
RD-2570	The system shall provide the capability for authorized users to search collections constrained by access rights.	Congressional Submission	Authorized User Search	R1C2 Must
RD-2573	The system shall provide the capability for authorized users to search for only work in progress content.	Congressional Submission	Authorized User Search	R1C3 Must
RD-2574	The system shall provide the capability for authorized users to search for work in progress content simultaneously with other content.	Congressional Submission	Authorized User Search	R1C3 Must
RD-2575	The system shall provide the capability for authorized users to search for only SIPs.	Congressional Submission	Authorized User Search	R1C2 Must
RD-2576	The system shall provide the capability for authorized users to search for SIPs simultaneously with other content.	Congressional Submission	Authorized User Search	R1C2 Must
RD-2577	The system shall provide the capability for authorized users to search for only AIPs.	Congressional Submission	Authorized User Search	R1C2 Must
RD-2578	The system shall provide the capability for authorized users to search for AIPs simultaneously with other content.	Congressional Submission	Authorized User Search	R1C2 Must
RD-2579	The system shall provide the capability for authorized users to search for only ACPs.	Congressional Submission	Authorized User Search	R1C2 Must
RD-2580	The system shall provide the capability for authorized users to search for ACPs simultaneously with other content.	Congressional Submission	Authorized User Search	R1C2 Must
RD-3696	The system shall provide the capability for Authorized Users to search by all fields in schema registered with the system.	Congressional Submission	Authorized User Search	R1C3 Must
RD-3701	The system shall provide the capability for authorized users to search collections constrained by user group.	Congressional Submission	Authorized User Search	R1C2 Must
RD-3702	The system shall provide the capability for Authorized Users to search jobs and by job BPI fields.	Congressional Submission	Authorized User Search	R1C3 Must
RD-3708	The system shall have the capability to allow authorized users to access content associated with a particular job or group of jobs from the search results.	Congressional Submission	Authorized User Search	R1C3 Must
RD-3709	The system shall have the capability to allow authorized users to access a job or jobs associated with a particular piece of content from the search results.	Congressional Submission	Authorized User Search	R1C3 Must
RD-407	The system shall have the capability to make automatic scope determinations.	Congressional Submission	Automatic Scope Determination	R1C3 Must
RD-462	The system shall have the capability to make automatic scope determinations based on metadata.	Congressional Submission	Automatic Scope Determination	R1C3 Must
RD-463	The system shall have the capability to make automatic scope determinations based on BPI.	Congressional Submission	Automatic Scope Determination	R1C3 Must
RD-208	The system shall provide the capability to support batch input of multiple digital objects and metadata for multiple publications.	Congressional Submission	Batch Submission of Content and Metadata	R1C2 Must
RD-3606	The system shall have the capability to associate the content and metadata submitted through batch submission with a job.	Congressional Submission	Batch Submission of Content and Metadata	R1C3 Must
RD-3607	The system shall have the capability to maintain the directory structure of batch submissions of content.	Congressional Submission	Batch Submission of Content and Metadata	R1C2 Must
RD-3608	The system shall have the capability to maintain the directory structure of batch submissions of metadata.	Congressional Submission	Batch Submission of Content and Metadata	R1C2 Must
RD-3609	The system shall provide the capability to support batch input of multiple digital objects and metadata for single publications.	Congressional Submission	Batch Submission of Content and Metadata	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1788	The system shall provide the capability to alert or notify the Congressional Content Originator that content has been successfully deposited in WIP.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-1789	The system shall provide the capability to alert or notify the Congressional Content Originator if content is not successfully deposited in WIP.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-1799	The system shall provide WIP storage for content prior to ingest.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-1928	The system shall accept digital content and metadata provided by Congressional Content Originators	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-1931	Deposited content user interface shall enable Congressional Content Originators to submit intended use information to the system.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-1932	Deposited content user interface shall enable Congressional Content Originators to submit approved for release information.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-1934	The system shall enable Congressional Content Originators to receive an alert or notification if content is not successfully deposited in WIP, explanation for why content was not deposited if available, and options for proceeding.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-2060	The system shall provide a user interface for Content Originator ordering.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-2213	The system shall provide the capability for users to request re-orders.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-2974	The system shall provide GUIs that accept submission of content by users.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-3029	The system must provide a default interface for GPO Service Specialists that is based on their user role.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C2 Must
RD-3610	The system shall accept digital content and metadata provided by GPO Service Specialists.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C2 Must
RD-3611	Congressional Content Submission GUIs shall conform to the specifications outlined in the Submission GUI Description (Congressional) Technical Memo	Congressional Submission	Congressional CO Submit Content and Metadata	R1C2 Must
RD-3612	The system shall allow Congressional Content Originators to view a manifest of submitted content through the user interface.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-3613	The system shall provide a GUI that allows Congressional Content Originators to submit content for Congressional Bills.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-3614	The system shall provide a GUI that allows Congressional Content Originators to submit content for ephemeral materials.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-3615	The system shall provide a GUI that allows GPO Service Specialists to submit content for Congressional Bills.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-3670	The system shall provide the capability for metadata to be edited by authorized users after submission to GPO.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C2 Must
RD-440	The system shall accept deposited content created without using style tools.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-454	The system shall have the capability to store content in WIP before job order information is received.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-475	The system shall have the capability to accept publisher approval information for SIP creation.	Congressional Submission	Congressional CO Submit Content and Metadata	R1C3 Must
RD-263	The system shall provide the capability to deliver content stored in an AIP regardless of the content's digital format.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-264	The system shall provide the capability for authorized users to access AIPs for the purpose of executing preservation processes or dissemination of DIPs from AIPs.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3346	The system shall have the capability to deliver files in their native application file format.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3348	The system shall have the capability to deliver optimized (print, press) PDFs.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3349	Optimized PDFs shall have fonts and images embedded.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3350	Image resolution of PDFs shall conform to industry best practices as defined in GPO's press optimized PDF settings.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3351	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3352	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files formatted in Adobe InDesign.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3353	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files formatted in QuarkXPress.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3354	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files formatted in Adobe FrameMaker.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3355	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files formatted in Adobe PageMaker.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3357	The system shall have the capability to deliver vector graphics.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3358	The system shall have the capability to deliver raster images.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3359	The system shall have the capability to deliver Microsoft Office Suite application files.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3360	The system shall have the capability to deliver Microsoft Office Suite application files in Microsoft Word.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3361	The system shall have the capability to deliver Microsoft Office Suite application files in Microsoft PowerPoint.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3362	The system shall have the capability to deliver Microsoft Office Suite application files in Microsoft Excel.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3363	The system shall have the capability to deliver Microsoft Office Suite application files in Microsoft Visio.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3364	The system shall have the capability to deliver XML.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3367	The system shall have the capability to deliver text files.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3368	The system shall have the capability to deliver text files in Rich Text (RTF) format.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3369	The system shall have the capability to deliver text files in ASCII text format.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3370	The system shall have the capability to deliver text files in Unicode format.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3371	The system shall have the capability to deliver text files in Universal Multi-Octet Coded Character Set that is equivalent to the native file.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3374	The system shall have the capability to deliver postscript files that are equivalent to the original files as ingested	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3408	The system shall have the capability to deliver electronic content in Microsoft PowerPoint File Format (.ppt) that is equivalent to the original file as ingested.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3409	The system shall have the capability to deliver electronic content in Microsoft Publisher File Format (.pub) that is equivalent to the original file as ingested.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3415	The system shall have the capability to deliver electronic content in TIFF that is equivalent to the original file as ingested.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3416	The system shall have the capability to deliver electronic content in GIF that is equivalent to the original file as ingested.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3417	The system shall have the capability to deliver electronic content in SVG conforming to Scalable Vector Graphic (SVG) 1.1 Specification that is equivalent to the original file as ingested.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3418	The system shall have the capability to deliver electronic content in EPS conforming to Encapsulated PostScript File Format Specification Version 3.0 that is equivalent to the original file as ingested.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3463	The system shall have the capability to deliver PIBs to GPO storage devices.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C3 Must
RD-3699	The system shall have the capability to deliver SGML files that are equivalent to the original files as ingested.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-3700	The system shall have the capability to deliver Locator files that are equivalent to the original files as ingested.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-396	The DIP shall have the capability to be an exact replica of the AIP.	Congressional Submission	Deliver Content and/or Metadata to Authorized Users	R1C2 Must
RD-1022	The system shall have the capability to alert or notify authorized users when duplicate content is rejected.	Congressional Submission	Duplicate Detection	R1C2 Must
RD-445	The system shall detect duplicate content in the system and alert or notify authorized users.	Congressional Submission	Duplicate Detection	R1C2 Must
RD-449	The system shall determine if the version of content is already in the system based on its content.	Congressional Submission	Duplicate Detection	R1C2 Must
RD-451	The system shall have the capability to reject duplicate content.	Congressional Submission	Duplicate Detection	R1C3 Must
RD-452	The system shall alert or notify authorized users when duplicate content is detected.	Congressional Submission	Duplicate Detection	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1937	Deposited content interface shall enable Internal Service Providers to submit digital content and metadata	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C2 Must
RD-3076	The system shall provide the capability for users to search context specific help menus	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C3 Must
RD-3616	The system shall allow Internal Service Providers to view a manifest of submitted content.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C2 Must
RD-3617	The system shall allow Internal Service providers to access content and metadata previously submitted by Congressional Content Originators.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C3 Must
RD-3618	The system shall have the capability to accept modified digital objects from the Internal Service Provider for Congressional Bills.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C3 Must
RD-3619	The system shall have the capability to accept modified packages from the Internal Service Provider for Congressional Bills.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C3 Must
RD-3620	The system shall provide a GUI for Internal Service Providers to manage renditions.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C2 Must
RD-3621	The system shall provide a GUI for internal Service Providers to submit new content for all collections currently on GPO Access to FDsys.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C2 Must
RD-3622	The system shall provide a GUI for Internal Service Providers to submit all Ephemeral content to FDsys.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C3 Must
RD-3623	The system shall provide a GUI for Internal Service Providers to submit new renditions of content.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C3 Must
RD-3663	The system shall have the capability to accept modified packages from the Internal Service Providers for Congressional Bills.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C3 Must
RD-3664	The system shall have the capability to accept modified digital objects from the Internal Service Providers for Congressional Bills.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C3 Must
RD-3667	The system shall provide a GUI for Internal Service Providers to delete work in progress renditions.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C3 Must
RD-3668	The system shall provide a GUI for Internal Service Providers to modify work in progress renditions.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C3 Must
RD-3669	The system shall provide a GUI for Internal Service Providers to enter metadata about work in progress renditions.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3703	The system shall provide the capability to notify or alert the Internal Service Provider that content submitted to FDsys was successfully ingested.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C2 Must
RD-3704	The system shall provide the capability to notify or alert the Internal Service Provider that content submitted to FDsys was not successfully ingested.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C2 Must
RD-3705	The system shall provide the capability to notify or alert the Internal Service Provider that content submitted to FDsys was not successfully ingested, explanation for why content was not ingested if available, and options for proceeding.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C2 Must
RD-3707	The system shall provide the capability to notify or alert the Internal Service Provider that content submitted to FDsys consisted of files that were not successfully ingested, explanation for why content files were not ingested if available, and options for proceeding.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C2 Must
RD-473	The system shall have the capability to accept modified packages from the Internal Service Provider after publisher approval for ephemeral materials.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C3 Must
RD-474	The system shall have the capability to accept modified digital objects from the Internal Service Provider after publisher approval for ephemeral materials.	Congressional Submission	Internal Service Provider Submit Content and Metadata	R1C3 Must
RD-1546	The system shall persist the BPI in a database with proper access controls to ensure data is not inadvertently changed.	Congressional Submission	Manage BPI	R1C3 Must
RD-2371	The system shall allow users to check out work in progress content and metadata.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-2372	The system shall not allow other users to modify content and metadata when a user has it checked out.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-2373	The system shall provide the capability to alert or notify authorized users when content and metadata has been checked out for longer than the allowed period defined by the work in progress workflow.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-2374	The system shall allow authorized users to release locks on content and metadata.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-2375	The system shall associate all versions of work in progress content.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-2376	The system shall allow users to check in content.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-3624	The system shall allow authorized users to assign jobs to other users.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-3625	The system shall allow authorized users to release check-in/check-out locks on jobs.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-3626	The system shall display to users that a job is checked out.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-3627	The system shall display to users which user has a job checked out.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-3628	The system shall provide the capability for an authorized Congressional Content Originators to approve content in WIP so it can be submitted to GPO.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-3629	The system shall not allow other users to modify job information when a user has the job checked out.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-3630	The system shall provide check in capabilities for jobs.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-3631	The system shall provide check out capabilities for jobs.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-3675	The system shall have the capability to provide access to all versions of stored work in progress content.	Congressional Submission	Manage Work In Progress	R1C3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3676	The system shall have the capability for an authorized Congressional Service Specialist to approve content in WIP so it can be submitted to GPO.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-3677	The system shall provide the capability to alert a user that tries to check out content or metadata that is already checked out.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-3678	The system shall provide the capability to alert a user that tries to check out a job that is already checked out.	Congressional Submission	Manage Work In Progress	R1C3 Must
RD-1803	The system shall unzip all zipped files and maintain the structure of directories and files.	Congressional Submission	Pre-Ingest Processing	R1C2 Must
RD-3253	The system shall have the capability to deliver pre-ingest bundles based on user requests.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3254	Users shall have the ability to pull DIPs and pre-ingest bundles from the system.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3258	The system shall provide the capability for a user to request the download of a PIB from the system.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3279	The system shall have the capability to assemble pre-ingest bundles containing digital objects, business process information and metadata required for service providers to output proofs and produce end product or service.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3280	The system shall have the capability to assemble pre-ingest bundles containing digital objects required for service providers to output proofs and produce end products or services.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3281	The system shall have the capability to assemble pre-ingest bundles containing BPI (job information) required for service providers to output proofs and produce end products or services.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3282	The system shall have the capability to assemble pre-ingest bundles containing metadata required for service providers to output proofs and produce end products or services.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3333	The system shall have the capability to deliver DIPs and pre-ingest bundles to users from which hard copy output can be created.	Congressional Submission	Pre-Ingest Processing	R1C2 Must
RD-3335	The system shall have the capability to provide DIPs from which hard copy can be created on any required hard copy output technology	Congressional Submission	Pre-Ingest Processing	R1C2 Must
RD-3336	The system shall have the capability to provide pre-ingest bundles from which hard copy can be created on any required hard copy output technology.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3435	The system shall have the capability to create pre-ingest bundles from content, BPI and metadata in such a way to support the transfer and copying to optical digital media.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3436	The system shall have the capability to create pre-ingest bundles from content, BPI and metadata in such a way to support the transfer and copying to Compact Discs (CD).	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3632	The system shall allow authorized users to designate the final, published versions of content in WIP that should be ingested into the system based upon content approval status.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3633	The system shall allow users to manually ingest final, published versions of content in WIP based upon content approval status.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3634	The system shall automatically ingest final, published versions of content in WIP based upon content approval status.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3635	The system shall have the capability to save PIB renditions in WIP.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3636	The system shall have the capability to store multiple versions of a PIB for the same job.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-3665	The system shall have the capability to create a manifest of submitted content.	Congressional Submission	Pre-Ingest Processing	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-390	The system shall have the capability for BPI (job information) to be associated with a DIP.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-472	The system shall have the capability to create pre-ingest bundles (PIB).	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-701	The system shall create and assign a unique ID for each job.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-702	The system shall provide the capability to assign a unique ID to each job.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-703	The system shall provide the capability to assign unique IDs to Content Originator orders of content jobs.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-704	The system shall provide the capability to assign unique IDs to Content Originator orders of service jobs.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-705	The system shall provide the capability to assign unique IDs to non-Content Originator order related jobs.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-706	The system shall not re-use Job unique IDs.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-721	The system shall allow the capability for an authorized user to input a CO supplied job tracking number.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-722	The system shall allow the capability for an authorized user to retrieve content and information about the content associated with a CO supplied job tracking number.	Congressional Submission	Pre-Ingest Processing	R1C3 Must
RD-2260	The system shall provide the capability for BPI to be rendered on the GPO Standard Form 1 (SF-1).	Congressional Submission	Render Job BPI on GPO Forms	R1C3 Must
RD-3638	The system shall provide the capability for BPI to be rendered on Pink Requisitions.	Congressional Submission	Render Job BPI on GPO Forms	R1C3 Must
RD-3681	The system shall provide the capability for BPI to be rendered on White Requisitions.	Congressional Submission	Render Job BPI on GPO Forms	R1C3 Must
RD-1857	Users shall have the capability to submit jobs prior to content being approved for ingest.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-1861	Authorized users shall have the capability to submit jobs prior to content being received by the system.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-1873	The system shall provide the capability to acquire BPI data on standard forms.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-1874	Authorized Users shall have the capability to enter data into BPI fields contained on Standard Forms.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-1875	The system shall provide the capability to edit BPI data on standard forms.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-1876	Users shall have the capability to enter data into BPI fields contained on the Standard Form 1.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-1877	The system shall provide the capability to store BPI data entered and edited by authorized users.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-1878	Authorized users shall have the capability to edit BPI fields contained on the Standard Form 1.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2064	The system shall have the capability to accept and store a Content Originator supplied job tracking number.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2065	The system shall have the capability to associate the Content Originator supplied job tracking number to the Job ID.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2078	The system shall provide the capability for a Content Originator to save BPI prior to submission to GPO.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2090	The system shall have the capability to alert or notify Service Specialists that a new job has been submitted by a Content Originator.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2091	The system shall have the capability to send jobs to appropriate Service Specialists based upon business rules.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2101	The system shall allow authorized users to specify a contract type.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2102	The system shall provide the capability for Content Originators to specify an existing contract (e.g., SPA, Term contract).	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2107	The system shall have the capability to allow Content Originators to enter an estimate when submitting a job.	Congressional Submission	Submit Congressional Jobs	R1C3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2108	The system shall have the capability to allow Service Specialists to enter an estimate when submitting a job.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2109	The system shall have the capability to allow Content Originators to enter a not to exceed price when submitting a job.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2111	The system shall have the capability for users to request a price approval.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2115	The system shall provide the capability for authorized users to edit BPI prior to submission to GPO.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2118	The system shall have the capability to save all BPI edits.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2126	The system shall provide the capability to enter multiple fulfillment destinations.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2127	The system shall allow users to upload distribution list of fulfillment destinations associated with a job.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2132	The system shall provide the capability for authorized users to select one ship date per fulfillment destination in a job.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2133	The system shall provide the capability for authorized users to select one delivery date per fulfillment destination in a job.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2134	The system shall provide the capability for authorized users to select one pickup date per fulfillment destination in a job.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2136	The system shall provide the capability for authorized users to download distribution list information.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2138	The system shall provide the capability for authorized users to select one mail date per fulfillment destination in a job.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2237	The system shall allow the capability for authorized users to attach files and a description of the files to a job.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-2238	The system shall have the capability to apply a timestamp to a job upon submission.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3496	The system shall have the capability to determine which jobs are sent to Service Specialists based upon business rules	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3497	The system shall have the capability to alert or notify Service Specialists that a new job has been received by the system	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3639	The system shall provide a specific GUI that allows congressional content originators to submit jobs for Congressional Bills.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3640	The system shall allow Congressional Content Originators to submit an open requisition.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3641	The system shall allow Service Specialists to submit an open requisition on behalf of a Content Originator.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3642	The system shall have the capability for authorized users to approve jobs in WIP so they can be submitted to GPO.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3644	The system shall have the capability to associate a job with an open requisition.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3645	The system shall provide a GUI that allows congressional users to submit jobs for ephemeral content.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3647	The system shall provide system announcements to Congressional Content Originators from authorized users.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3648	The system shall provide the capability for users to delete miscellaneous information which will be saved on their homepage.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3649	The system shall provide the capability for users to edit miscellaneous information which will be saved on their homepage.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3650	The system shall provide the capability for users to enter miscellaneous information which will be saved on their homepage.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3651	The system shall provide the capability for users to enter notes for individual Congressional Bills	Congressional Submission	Submit Congressional Jobs	R1C3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3652	The system shall provide the capability for users to enter notes for individual Congressional jobs for ephemeral material.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3653	The system shall provide the capability for users to request an electronic proof on the ephemeral submission GUI.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3654	The system shall provide the capability for Content Originators to enter BPI data specific fields contained on Pink Requisitions	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3655	The system shall provide the capability for Content Originators to edit BPI data specific fields contained on Pink Requisitions	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3656	The system shall provide the capability to store BPI data specific fields contained on Pink Requisitions	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3657	The system shall provide user generated announcements to Congressional Content Originators based upon alerts or notifications.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3680	The system shall be capable of providing a summarized view of BPI for a job.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3682	The system shall have the capability to alert Congressional Content Originators that a Content Originator supplied job tracking number has been used previously by that Congressional CO.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3684	The system shall alert users if they select a fulfillment date that has already passed.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3685	The system shall display job action information to authorized users.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3686	The system shall have the capability to associate a batch submission of jobs with an open requisition.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3692	The system shall have the capability to accept data from the Congressional Member Database.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3693	The system shall have the capability to manage data collected from the Congressional Member Database in a user's profile.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3695	The system shall have the capability to alert users that CO supplied job tracking number has been used previously by that agency.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3712	The system shall have the capability to alert or notify Internal Service Providers that a new job has been received by the system	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3714	The system shall provide the ability for authorized users to order jobs from term contracts from which they are authorized to purchase against.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3716	The system shall provide the ability for authorized users to order jobs from open requisitions from which they are authorized to purchase against.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3717	The system shall provide the capability to manage open requisitions and who is authorized to place jobs on them.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-460	The system shall associate jobs BPI with corresponding content and metadata.	Congressional Submission	Submit Congressional Jobs	R1C3 Must
RD-3671	Deposited content user interface shall provide alerts or notifications to Congressional Content Originators of receipt of content.	Congressional Submission	Submit Content and Metadata	R1C3 Must
RD-3672	The system shall provide alerts or notifications to Congressional Content Originators if content related to a job is not received in WIP, explanation for why content was not received if available, and options for proceeding.	Congressional Submission	Submit Content and Metadata	R1C3 Must
RD-3691	The system shall provide the capability to alert or notify the Congressional Content Originator that content submitted to FDsys consisted of files that were not successfully ingested, explanation for why content files were not ingested if available, and options for proceeding.	Congressional Submission	Submit Content and Metadata	R1C3 Must
RD-1865	The system shall have the capability to track job submission status using the job ID.	Congressional Submission	Track Jobs	R1C3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2103	The system shall allow authorized users to view a history of all previous jobs based on user rights.	Congressional Submission	Track Jobs	R1C3 Must
RD-2104	The system shall allow authorized users to see all of the jobs for the group(s) that they belong to.	Congressional Submission	Track Jobs	R1C3 Must
RD-2215	The system shall have the capability for an authorized user to inform the system that they have completed an activity.	Congressional Submission	Track Jobs	R1C3 Must
RD-3637	The system shall provide the capability for users to delete content in WIP.	Congressional Submission	Track Jobs	R1C3 Must
RD-3658	The system shall allow Congressional Content Originators to view status information about job activities.	Congressional Submission	Track Jobs	R1C3 Must
RD-3659	The system shall allow GPO users to add status information about job activities.	Congressional Submission	Track Jobs	R1C3 Must
RD-3660	The system shall allow GPO users to delete status information about job activities.	Congressional Submission	Track Jobs	R1C3 Must
RD-3661	The system shall allow GPO users to modify status information about job activities.	Congressional Submission	Track Jobs	R1C3 Must
RD-3662	The system shall allow users to associate status information about job activities with content in WIP.	Congressional Submission	Track Jobs	R1C3 Must
RD-3666	The system shall provide a GUI for Internal Service Providers to delete work in progress renditions.	Congressional Submission	Track Jobs	R1C3 Must
RD-3694	The system shall have the capability to track job submission status using the CO supplied job tracking number.	Congressional Submission	Track Jobs	R1C3 Must
RD-3706	The system shall provide the capability to notify or alert the Internal Service Provider that content submitted to FDsys consisted of files that were successfully ingested and files that were not successfully ingested.	Congressional Submission	Track Jobs	R1C2 Must

3.4 CONTENT SUBMISSION FEATURE GROUP REQUIREMENTS

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2965	The system shall provide a default Service Specialist workbench that provides the capability for Service Specialists to handle exception processing.	Content Submission	Congressional CO Submit Content and Metadata	R1C4 Must
RD-2209	The system shall allow authorized users to request contract modifications.	Content Submission	Content Submission	R2 Should / R3 Must
RD-430	The DIP shall have the capability to include Business Process Information, including information collected about orders from the CO Ordering function and requests made by end users.	Content Submission	Deliver Content and/or Metadata	R2 Must
RD-3365	The system shall support cascading style sheets.	Content Submission	Deliver Content and/or Metadata to Authorized Users	R1C4 Must
RD-3366	The system shall support document type definition/schema.	Content Submission	Deliver Content and/or Metadata to Authorized Users	R1C4 Must
RD-3373	The system shall have the capability to deliver OASIS Open Document Format for Office Applications (OpenDocument) v1.0.	Content Submission	Deliver Content and/or Metadata to Authorized Users	R1C4 Must
RD-3414	The system shall have the capability to deliver electronic content in JPEG 2000 that is equivalent to the original file as ingested.	Content Submission	Deliver Content and/or Metadata to Authorized Users	R1C4 Must
RD-3466	The system shall have the capability to deliver PIBs to non-GPO storage devices.	Content Submission	Deliver Content and/or Metadata to Authorized Users	R1C4 Must
RD-447	The system shall determine if the version of content is already in the system using version information.	Content Submission	Duplicate Detection	R1C4 Must
RD-448	The system shall determine if the version of content is already in the system using bibliographic information.	Content Submission	Duplicate Detection	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1794	The system shall have the capability to allow users to specify what the intended use and access rights to the content should be.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1795	The system shall have the capability to allow users to specify what the intended distribution of the content should be.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1797	The system shall have the capability to notify authorized users that copyrighted content has been submitted.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1805	The system shall accept content with specialized character sets (e.g., non-Roman, scientific notations)	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1827	The system shall record or ascertain elements relating to documents.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1828	The system shall record the software applications and versions used to create the digital objects.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1888	The system shall record the page size of the publication.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1889	The system shall record the trim size of the publication.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1890	The system shall record the number of pages.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1891	The system shall record the file formats.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1892	The system shall record file sizes.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1893	The system shall record what fonts are used in the publication.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1894	The system shall record if the fonts are furnished or embedded.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1895	The system shall record font types.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1896	The system shall record what color mode(s) are used in the publication.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1897	The system shall record whether bleed is required/provided for.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1898	The system shall record information about the construction of a publication.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1899	The system shall record image resolutions.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1903	The system shall record or ascertain elements relating to audio.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1904	The system shall record audio file formats.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1905	The system shall record the size of audio files.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1906	The system shall record audio playing time.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1907	The system shall record the language of audio.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1908	The system shall record audio file compression information.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1909	The system shall support the capability to record the bit rate of audio.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1912	The system shall record video file formats.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1913	The system shall record video files sizes.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1914	The system shall record closed captioning information.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1915	The system shall record video runtime.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1916	The system shall record video encoding scheme.	Content Submission	Enter BPI and Metadata	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1917	The system shall record the language of the video.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-1918	The system shall record video file compression information.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-2077	The system shall allow authorized users to add new BPI fields.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-2093	The system shall have the capability for Content Evaluators to add rider information to BPI.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-2114	The system shall provide the capability for authorized users to edit BPI prior to contract award.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-2116	The system shall have the capability to display BPI edits.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-2117	The system shall have the capability to display the user name of who edited BPI.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-2119	The system shall have the capability to notify users that BPI for a job has been edited.	Content Submission	Enter BPI and Metadata	R1C4 Must
RD-3030	The system must provide a workbench for Service Providers (e.g., GPO Service Providers and External Service Providers) that is based on their user role.	Content Submission	Internal Service Provider Submit Content and Metadata	R1C4 Must
RD-3259	The system shall provide the capability for a user to perform an FTP get on a PIB from the system.	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-3308	The system shall have the capability to push PIBs to users using E-mail.	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-3309	Users shall have the capability to request an e-mail of a PIB for a single order they have been awarded.	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-3311	The system shall have the capability to push PIBs to users using File Transfer Protocol.	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-3312	Users shall have the capability to request an FTP of a PIB for a single order they have been awarded.	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-3317	The maximum size PIB delivered by HTTP download shall be configurable by an authorized user.	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-3321	The maximum size PIB delivered by e-mail shall be configurable by an authorized user.	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-3323	The maximum size PIB delivered by FTP shall be configurable by an authorized user.	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-3438	The system shall have the capability to create pre-ingest bundles from content, BPI and metadata in such a way to support the transfer and copying to Digital Versatile Disc (DVD)	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-3441	The system shall have the capability to create pre-ingest bundles from content, BPI and metadata in such a way to support the transfer and copying to Blue Ray Discs (BD).	Content Submission	Pre-Ingest Processing	R1C4 Could
RD-3443	The system shall have the capability to deliver pre-ingest bundles that are portable (i.e. can be viewed on other systems) via magnetic tapes supported by the client environment.	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-3444	The system shall have the capability to deliver pre-ingest bundles that are portable (i.e., can be viewed on other systems) via magnetic hard disks supported by the client environment.	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-3445	The system shall have the capability to deliver pre-ingest bundles that are portable (i.e., can be viewed on other systems) via magnetic floppy disks supported by the client environment.	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-3449	The system shall have the capability to deliver pre-ingest bundles that are portable (i.e., can be viewed on other systems) via removable semiconductor digital media supported by the client environment.	Content Submission	Pre-Ingest Processing	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3450	The system shall have the capability to deliver pre-ingest bundles that are portable (i.e., can be viewed on other systems) via Universal Serial Bus (USB) flash drives supported by the client environment.	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-3451	The system shall have the capability to deliver pre-ingest bundles that are portable (i.e., can be viewed on other systems) via flash memory cards supported by the client environment.	Content Submission	Pre-Ingest Processing	R1C4 Must
RD-441	The system shall accept deposited content created using style tools.	Content Submission	Pre-Ingest Processing	R2 Could / R3 Must
RD-450	The system shall have the capability to detect near duplicate documents.	Content Submission	Pre-Ingest Processing	R3 Must
RD-2261	The system shall provide the capability for BPI to be rendered on the GPO Form 952.	Content Submission	Render Job BPI on GPO Forms	R1C4 Must
RD-2262	The system shall provide the capability for BPI to be rendered on the GPO Form 2511.	Content Submission	Render Job BPI on GPO Forms	R1C4 Must
RD-2263	The system shall provide the capability for BPI to be rendered on the GPO Form 3868.	Content Submission	Render Job BPI on GPO Forms	R1C4 Must
RD-3679	The system shall provide the capability for BPI to be rendered on the GPO Standard Form 3000 (SF-3000).	Content Submission	Render Job BPI on GPO Forms	R1C4 Must
RD-3028	The system must provide a workbench for GPO Content Evaluators that is based on their user role.	Content Submission	Scope Determination	R1C4 Must
RD-461	The system shall allow Content Evaluators to make scope determinations.	Content Submission	Scope Determination	R1C4 Must
RD-464	The system shall have the capability to make automatic scope determinations based on content.	Content Submission	Scope Determination	R3 Must
RD-465	The system shall allow users to modify the criteria by which the system makes automatic scope determinations.	Content Submission	Scope Determination	R1C4 Must
RD-466	The system shall provide a GUI interface for users to modify the criteria for automatic scope determinations.	Content Submission	Scope Determination	R2 Must
RD-3713	The system shall have the capability to determine which jobs are sent to Internal Service Providers based upon business rules	Content Submission	Submit Congressional Jobs	R1C4 Must
RD-1793	The system shall have the capability to allow users to indicate that content contains copyrighted material.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-1804	Stuffed files (.sit) shall be unstuffed.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-1923	The system shall accept digital content and metadata provided by Content Originators.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-1935	The system shall have the capability to notify Congressional Content Originators that their content has been released.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-1944	The system shall have capability to accept converted content.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-1952	Manage converted content	Content Submission	Submit Content and Metadata	R1C4 Must
RD-3687	The system shall provide the capability to alert or notify the Congressional Content Originator that content submitted to FDsys was successfully ingested.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-3688	The system shall provide the capability to alert or notify the Congressional Content Originator that content submitted to FDsys was not successfully ingested.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-3689	The system shall provide the capability to alert or notify the Congressional Content Originator that content submitted to FDsys was not successfully ingested, explanation for why content was not ingested if available, and options for proceeding.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-3690	The system shall provide the capability to alert or notify the Congressional Content Originator that content submitted to FDsys consisted of files that were successfully ingested and files that were not successfully ingested.	Content Submission	Submit Content and Metadata	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-442	The system shall accept converted content.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-443	The system shall accept harvested content.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-812	The system shall provide the capability to verify and validate the authenticity, integrity, and official status of converted content.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-813	The system shall provide the capability to validate the authenticity of converted content.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-814	The system shall provide the capability to validate the integrity of converted content.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-815	The system shall provide the capability to validate the official status of converted content.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-818	The system shall ensure that converted content has not been altered or destroyed in an unauthorized manner during transmission from authorized users to the system, and information about content integrity should be recorded in metadata.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-819	The system shall validate that converted content has not been altered in an unauthorized manner during transmission to the system.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-820	The system shall validate that converted content has not been destroyed in an unauthorized manner during transmission to the system.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-821	The system shall record information about converted content integrity in metadata.	Content Submission	Submit Content and Metadata	R1C4 Must
RD-835	The system shall provide the capability to process encrypted files at pre-ingest.	Content Submission	Submit Content and Metadata	R2 Must
RD-1790	The system shall have the capability to provide notification to the submission agency/authority that the content has been released to the intended users.	Content Submission	Submit Jobs	R1C4 Must
RD-1879	The system shall provide the capability to acquire BPI data specific fields contained on the GPO Form 952.	Content Submission	Submit Jobs	R1C4 Must
RD-1880	The system shall provide the capability to store BPI data specific fields contained on the GPO Form 952.	Content Submission	Submit Jobs	R1C4 Must
RD-1881	The system shall provide the capability to edit BPI data specific fields contained on the GPO Form 952.	Content Submission	Submit Jobs	R1C4 Must
RD-1882	The system shall provide the capability to acquire BPI data specific fields contained on the GPO Form 2511.	Content Submission	Submit Jobs	R1C4 Must
RD-1883	The system shall provide the capability to store BPI data specific fields contained on the GPO Form 2511.	Content Submission	Submit Jobs	R1C4 Must
RD-1884	The system shall provide the capability to edit BPI data specific fields contained on the GPO Form 2511.	Content Submission	Submit Jobs	R1C4 Must
RD-1885	The system shall provide the capability to acquire BPI data specific fields contained on the GPO Form 3868.	Content Submission	Submit Jobs	R1C4 Must
RD-1886	The system shall provide the capability to store BPI data specific fields contained on the GPO Form 3868.	Content Submission	Submit Jobs	R1C4 Must
RD-1887	The system shall provide the capability to edit BPI data specific fields contained on the GPO Form 3868.	Content Submission	Submit Jobs	R1C4 Must
RD-1945	Digital content may be provided in file formats for digitized tangible documents as specified in Appendix B: Operational Specification for Converted Content.	Content Submission	Submit Jobs	R1C4 Must
RD-1947	Converted content interface shall enable GPO Service Providers and external Service Providers to:	Content Submission	Submit Jobs	R1C4 Must
RD-1948	Submit approved content and metadata.	Content Submission	Submit Jobs	R1C4 Must
RD-1949	Receive notification of receipt of content and content ID	Content Submission	Submit Jobs	R1C4 Must
RD-1950	Provide notification of release of content	Content Submission	Submit Jobs	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1951	Receive notification if content is not received, explanation for why content was not received, and options for proceeding	Content Submission	Submit Jobs	R1C4 Must
RD-2066	The system shall allow authorized users to update the Content Originator supplied job tracking number at any time.	Content Submission	Submit Jobs	R1C4 Must
RD-2067	The system shall have the capability to alert authorized users that a Content Originator supplied job tracking number has been updated.	Content Submission	Submit Jobs	R1C4 Must
RD-2074	The system shall provide the capability to acquire, store and edit BPI data specific fields contained on the GPO Form 952.	Content Submission	Submit Jobs	R1C4 Must
RD-2075	The system shall provide the capability to acquire, store and edit BPI data specific fields contained on the GPO Form 2511.	Content Submission	Submit Jobs	R1C4 Must
RD-2076	The system shall provide the capability to acquire, store and edit BPI data specific fields contained on the GPO Form 3868.	Content Submission	Submit Jobs	R1C4 Must
RD-2089	The system shall have the capability to allow users to indicate that two or more jobs should be strapped.	Content Submission	Submit Jobs	R1C4 Must
RD-2094	The system shall have the capability to add Content Evaluator rider quantity information to the Content Originator job.	Content Submission	Submit Jobs	R1C4 Must
RD-2095	The system shall have the capability to add Content Evaluator rider fulfillment information to the Content Originator job.	Content Submission	Submit Jobs	R1C4 Must
RD-2096	The system shall have the capability to add Content Evaluator rider billing information to the Content Originator job.	Content Submission	Submit Jobs	R1C4 Must
RD-2130	The system shall provide the capability for users to store fulfillment destinations in their user profile.	Content Submission	Submit Jobs	R1C4 Must
RD-3271	The system shall have the capability to alert or notify users of fulfillment.	Content Submission	Submit Jobs	R1C4 Must
RD-3643	The system shall have the capability to associate a job with a term contract.	Content Submission	Submit Jobs	R1C4 Must
RD-3646	The system shall provide job-specific, system generated “Upcoming Events” information based upon business rules and alerts and notifications.	Content Submission	Submit Jobs	R1C4 Must
RD-3673	The system shall have the capability to alert Content Evaluators that a new job has been submitted by a Content Originator.	Content Submission	Submit Jobs	R1C4 Must
RD-3674	The system shall have the capability to send jobs to appropriate Content Evaluators based upon business rules.	Content Submission	Submit Jobs	R1C4 Must
RD-3683	The system shall provide the capability for users to create groups of fulfillment destinations in their profile.	Content Submission	Submit Jobs	R1C4 Must
RD-3710	The system shall have the capability to alert or notify Content Evaluators that a new job has been received by the system	Content Submission	Submit Jobs	R1C4 Must
RD-3711	The system shall have the capability to determine which jobs are sent to Content Evaluators based upon business rules	Content Submission	Submit Jobs	R1C4 Must
RD-3715	The system shall provide the capability to manage term contracts and who is authorized to place jobs on them.	Content Submission	Submit Jobs	R1C4 Must
RD-1858	Users shall have the capability to write specifications for jobs prior to content being approved for ingest.	Content Submission		R3 Must
RD-1859	Users shall have the capability to award jobs prior to content being approved for ingest.	Content Submission		R3 Must
RD-1860	Users shall have the capability to send awarded jobs to service providers prior to content being approved for ingest.	Content Submission		R3 Must
RD-1862	Users shall have the capability to write specifications for jobs prior to content being received.	Content Submission		R3 Must
RD-1863	Users shall have the capability to award jobs prior to content being received.	Content Submission		R3 Must
RD-1864	Users shall have the capability to send awarded jobs to service providers prior to content being received.	Content Submission		R3 Must
RD-1867	The system shall have the capability to interface with select external agency systems in order to accept content.	Content Submission		R3 Could
RD-1868	The system shall provide the capability to write specifications for jobs	Content Submission		R3 Must
RD-1869	The system shall provide the capability to create common phrases used in specifications.	Content Submission		R3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1870	The system shall provide the capability to save common phrases used in specifications.	Content Submission		R3 Must
RD-1871	The system shall provide the capability to edit common phrases used in specifications.	Content Submission		R3 Must
RD-1872	The system shall provide the capability to insert common phrases into specifications.	Content Submission		R3 Must
RD-1955	The system shall accept digital content and metadata delivered by the harvesting function.	Content Submission		R2 Must
RD-1957	The system shall provide the capability to record the date and time of harvest of content.	Content Submission		R2 Must
RD-1959	The harvester shall have the capability to discover, assess, and harvest in-scope content from targeted Web sites.	Content Submission		R2 Must
RD-1960	The harvester shall have the capability to ensure that it does not harvest the same content more than once.	Content Submission		R2 Must
RD-1961	The harvester shall have the capability to perform the discovery, assessment, and harvesting processes on target Web sites based on update schedules.	Content Submission		R2 Must
RD-1962	The harvester shall have capability to perform simultaneous harvests.	Content Submission		R2 Must
RD-1963	The harvester shall locate and harvest all levels of Web pages within a Web site.	Content Submission		R2 Must
RD-1964	The harvester shall go outside the target domains or Web sites only when the external domain contains in-scope content.	Content Submission		R2 Must
RD-1965	The harvester shall stop the discovery process when a Robots.txt is present and prevents the harvester from accessing a Web directory, consistent with GPO business rules.	Content Submission		R2 Must
RD-1966	The harvester shall stop the discovery process when a linked Web page does not contain in-scope content.	Content Submission		R2 Must
RD-1967	The harvester shall flag content and URLs that are only partially harvested by the automated harvester for manual follow-up.	Content Submission		R2 Must
RD-1968	The harvester shall determine if the discovered content is within the scope of GPO dissemination programs as defined in 44USC1901, 1902, 1903, and by GPO.	Content Submission		R2 Must
RD-1969	The harvester shall collect in-scope discovered content and available metadata.	Content Submission		R2 Must
RD-1970	The harvester shall deliver all in-scope content and metadata to WIP storage.	Content Submission		R2 Must
RD-1971	The harvester shall have the ability to discover and collect all file types that may reside on target Web sites.	Content Submission		R2 Must
RD-1972	The harvester shall be able to harvest and transfer a complete, fully faithful copy of the original content (e.g., publication, digital object, audio and video streams).	Content Submission		R2 Must
RD-1973	The harvester shall have the ability to maintain the directory structure of Web sites that constitute entire publications.	Content Submission		R2 Must
RD-1974	The harvester shall have the capability to re-configure directory structures of harvested content based on GPO rules and instructions (e.g., all PDF files are placed in one folder).	Content Submission		R2 Must
RD-1975	The harvester shall be able to harvest hidden Web information.	Content Submission		R2 Must
RD-1976	The harvester shall be able to harvest content contained in query-based databases.	Content Submission		R2 Must
RD-1977	The harvester shall be able to harvest content contained in agency content management systems.	Content Submission		R2 Must
RD-1978	The harvester shall be able to harvest content contained on dynamically generated Web pages.	Content Submission		R2 Must
RD-1979	The harvester shall be able to harvest content contained on FTP servers.	Content Submission		R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1980	The harvester shall be able to harvest content contained behind proxy servers.	Content Submission		R2 Must
RD-1981	The harvester shall be able to harvest content contained behind firewalls.	Content Submission		R2 Must
RD-1982	The harvester shall provide the capability to automatically route specific content for which scope determinations could not be made to Content Evaluators. These situations include, but are not limited to: . Content that could not be reached by the harvester (e.g., content behind robots.txt files and firewalls, restricted access databases, etc). . Duplicate content that appears on more than one official Federal Government Web site. . Content for which not enough information or metadata exists to make scope determinations based on harvester rules and instructions alone.	Content Submission		R2 Must
RD-1983	The harvester shall have the capability to time and date stamp content that has been harvested.	Content Submission		R2 Must
RD-1985	The harvester shall have the ability to locate and collect all metadata associated with harvested content, including identity, responsibility, reference information, version/fixity, technical, administrative and life cycle dates.	Content Submission		R2 Must
RD-1986	The harvester shall have the ability to locate and collect unique ID and title/caption information.	Content Submission		R2 Must
RD-1987	The harvester shall have the ability to locate and collect author/creator, publisher/authority, and rights owner information.	Content Submission		R2 Must
RD-1988	The harvester shall have the ability to locate and collect topical information and bibliographic descriptions.	Content Submission		R2 Must
RD-1989	The harvester shall have the ability to locate and collect version, fixity, relationship, and provenance information.	Content Submission		R2 Must
RD-1990	The harvester shall have the ability to locate and collect technical, structural, file format, packaging and representation information.	Content Submission		R2 Must
RD-1991	The harvester shall have the ability to locate and collect administrative metadata	Content Submission		R2 Must
RD-1992	The harvester shall have the capability to record the time and date of harvest.	Content Submission		R2 Must
RD-1994	The harvester shall discover and identify Federal content (e.g., publications, digital objects, audio and video) on Web sites using criteria specified by GPO Business Units.	Content Submission		R2 Must
RD-1995	The harvester shall accept and apply rules and instructions that will be used to assess whether discovered content is within scope of GPO dissemination programs.	Content Submission		R2 Must
RD-1996	The harvester shall be able to create and store rule and instruction profiles for individual targeted Web sites.	Content Submission		R2 Must
RD-1998	The harvester shall provide a user interface to accommodate workflow management and scheduling of harvesting activities.	Content Submission		R2 Must
RD-1999	The user interface shall allow authorized users (GPO-specified) to schedule harvesting activities based on update schedules for targeted sites to be harvested.	Content Submission		R2 Must
RD-2000	Shall accommodate the scheduling of harvests, including but not limited to hourly, daily, weekly, biweekly, monthly, and yearly.	Content Submission		R2 Must
RD-2001	The user interface shall be able to manage rule and instruction profiles.	Content Submission		R2 Must
RD-2003	The harvester shall provide quality control functions to test accuracy/precision of rule application.	Content Submission		R2 Must
RD-2004	The harvester shall be able to incorporate results of quality control functions into rule and instruction creation/refinement.	Content Submission		R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2005	The harvester shall have the capability to log and produce reports on harvesting activities.	Content Submission		R2 Must
RD-2006	The harvester shall have the capability to log and report on Web sites visited by the harvester (e.g., date, time, frequency).	Content Submission		R2 Must
RD-2007	The harvester shall have the capability to log and report on content discovered, including location, title, description, and other relevant information.	Content Submission		R2 Must
RD-2008	The harvester shall have the capability to log and report on scope assessment decisions made by the harvester.	Content Submission		R2 Must
RD-2009	The harvester shall have the capability to log and report on target Web site structure, hierarchy, relationships, and directories.	Content Submission		R2 Must
RD-2010	The harvester shall have the capability to log and report on harvester failure or error rates (e.g. network problems, broken links, security rules, firewalls, corrupted content).	Content Submission		R2 Must
RD-2011	The harvester shall have the capability to log harvester failure or error rates (e.g. network problems, broken links, security rules, firewalls, corrupted content).	Content Submission		R2 Must
RD-2012	The harvester shall have the capability to report on harvester failure or error rates (e.g. network problems, broken links, security rules, firewalls, corrupted content).	Content Submission		R2 Must
RD-2013	The harvester shall have the capability to log and report comparing target Web sites at different points in time (e.g., different times of harvest)	Content Submission		R2 Must
RD-2014	The discovery and harvesting tools shall have the ability to identify GPO as the owner of the tools.	Content Submission		R2 Must
RD-2015	The harvester's method of identification shall not be intrusive to targeted Web site.	Content Submission		R2 Must
RD-2016	The harvester shall have the ability to collect integrity marks associated with content as it is being harvested.	Content Submission		R2 Must
RD-2019	Style tools shall accept content from authorized Content Originators, Service Providers, and Service Specialists for document creation.	Content Submission		R2 Could / R3 Must
RD-2020	Style tools shall accept metadata from authorized users (e.g., title, author).	Content Submission		R2 Could / R3 Must
RD-2021	Style tools shall provide the capability for users to create new content for document creation.	Content Submission		R2 Could / R3 Must
RD-2022	Style tools shall provide the capability for users to compose content for document creation including but not limited to text, images, and graphics.	Content Submission		R2 Could / R3 Must
RD-2023	Style tools shall allow users to compose content based on pre-defined design rules.	Content Submission		R2 Could / R3 Must
RD-2024	Style tools shall allow users to compose content using templates based on rules (e.g., agency style manuals).	Content Submission		R2 Could / R3 Must
RD-2025	Style tools shall have the capability to prompt users to define layout parameters from best available or system presented options.	Content Submission		R2 Could / R3 Must
RD-2026	Style tools shall allow multiple users to work collaboratively on the same content, prior to publication.	Content Submission		R2 Could / R3 Must
RD-2027	Style tools shall allow authorized users to approve/reject content changes made by collaborators.	Content Submission		R2 Could / R3 Must
RD-2028	Style tools shall track approval/rejection of changes to content, prior to publication.	Content Submission		R2 Could / R3 Must
RD-2029	Style tools shall allow for approval of content.	Content Submission		R2 Could / R3 Must
RD-2030	Style tools shall allow for approval of content presentation.	Content Submission		R2 Could / R3 Must
RD-2031	Style tools shall provide the capability to revert to a previously saved version of a working file (e.g., History palette).	Content Submission		R2 Could / R3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2032	Style tools shall provide the capability to track and undo changes to WIP content.	Content Submission		R2 Could / R3 Must
RD-2033	Style tools shall allow users to select output methods for viewing preliminary composition (i.e. Preparatory representation of content format or structure).	Content Submission		R2 Could / R3 Must
RD-2034	Style tools shall interface with Content Originator ordering.	Content Submission		R2 Could / R3 Must
RD-2036	Style tools shall have the capability to automatically compose content.	Content Submission		R2 Could / R3 Must
RD-2037	Style tools shall have the capability to automatically compose content and place graphical elements in locations using GPO or Agency guidelines.	Content Submission		R2 Could / R3 Must
RD-2038	Style tools shall have the capability to automatically compose content based on user preferences.	Content Submission		R2 Could / R3 Must
RD-2039	Style tools shall have the capability to automatically compose content based on content analysis.	Content Submission		R2 Could / R3 Must
RD-2040	Style tools shall allow users to modify automatically composed content.	Content Submission		R2 Could / R3 Must
RD-2042	The system shall accept content based on the access rights and privileges of the user submitting the content.	Content Submission		R2 Could / R3 Must
RD-2043	The system shall assign unique IDs to digital objects created by style tools.	Content Submission		R2 Could / R3 Must
RD-2044	The system shall provide storage for WIP style tools content.	Content Submission		R2 Could / R3 Must
RD-2045	The system shall allow management of WIP content based on access rights and privileges.	Content Submission		R2 Could / R3 Must
RD-2046	The system shall provide tracking of all WIP activities.	Content Submission		R2 Could / R3 Must
RD-2047	The system shall provide search and retrieval capabilities for WIP content.	Content Submission		R2 Could / R3 Must
RD-2048	The system shall provide search and retrieval capabilities for content stored within ACP storage (e.g., to allow Content Originators to pull unique digital objects into the style tools creative process).	Content Submission		R2 Could / R3 Must
RD-2049	The system shall have the capability to provide authorized users with the ability to cancel a job.	Content Submission		R2 Should /R3 Must
RD-2050	The system shall have the capability to send or log notification of fulfillment to single or multiple users.	Content Submission		R2 Should /R3 Must
RD-2051	The system shall have the capability to provide notification of fulfillment based on the log of activities.	Content Submission		R2 Should /R3 Must
RD-2052	The system shall have the capability for users to specify the methods in which they receive fulfillment notification (e.g., email, alerts).	Content Submission		R2 Should /R3 Must
RD-2053	The system shall have the capability for users to elect not to receive notification of fulfillment.	Content Submission		R2 Should /R3 Must
RD-2054	The system shall allow authorized users to manage fulfillment notification.	Content Submission		R2 Should /R3 Must
RD-2055	The system shall have the capability to store multiple tracking numbers for each order.	Content Submission		R2 Should /R3 Must
RD-2056	The system shall provide a hyperlink to a fulfillment provider tracking website.	Content Submission		R2 Should /R3 Must
RD-2057	The system shall have the capability to receive multiple confirmations of fulfillment.	Content Submission		R2 Should /R3 Must
RD-2061	The system shall have the capability to process jobs prior to content being approved for ingest.	Content Submission		R3 Must
RD-2062	The system shall have the capability to process jobs prior to content being received.	Content Submission		R3 Must
RD-2063	The system shall have the capability to track jobs using the job ID.	Content Submission		R3 Must
RD-2069	The system shall have the capability to interface with select external agency systems in order to retrieve jobs.	Content Submission		R3 Could

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2070	The system shall adhere to policies set forth in GPO Publication 305.3.	Content Submission		R3 Must
RD-2084	The system shall provide the capability for users to search all job specifications.	Content Submission		R3 Must
RD-2085	The system shall provide the capability for users to search job specifications related to a user account or agency.	Content Submission		R3 Must
RD-2086	The system shall have the capability to strap jobs.	Content Submission		R3 Must
RD-2087	The system shall have the capability to detect similar jobs that have not been awarded for the purpose of strapping.	Content Submission		R3 Could
RD-2088	The system shall have the capability to notify users of similar jobs that have not been awarded for the purpose of strapping.	Content Submission		R3 Could
RD-2092	The system shall have the capability to support job riders.	Content Submission		R2 Should / R3 Must
RD-2097	The system shall have the capability for users to submit rider information to GPO.	Content Submission		R2 Should /R3 Must
RD-2098	The system shall provide the capability to notify authorized users that riders have been placed on their job.	Content Submission		R2 Should /R3 Must
RD-2099	The system shall provide the capability to notify users that GPO is accepting riders for a job.	Content Submission		R2 Should / R3 Must
RD-2100	The system shall have the capability to determine contract types (e.g., onetime bids, SPA, term contract) based upon BPI and business rules.	Content Submission		R3 Could
RD-2105	The system shall provide estimated costs for GPO products and services for jobs to users based upon user provided BPI.	Content Submission		R2 Should /R3 Must
RD-2110	The system shall have the capability to allow authorized users to provide an estimate for a job.	Content Submission		R3 Must
RD-2112	The system shall have the capability for users to approve/disapprove a price.	Content Submission		R3 Must
RD-2113	The system shall provide the capability for authorized users to edit job specifications prior to contract award.	Content Submission		R3 Must
RD-2124	The system shall allow users to select fulfillment options for content delivery.	Content Submission		R3 Must
RD-2125	The system shall provide the capability to configure the tangible content delivery options.	Content Submission		R3 Must
RD-2128	The system shall compile fulfillment destination into multiple standardized formats.	Content Submission		R3 Must
RD-2129	The system shall be capable of extracting fulfillment destinations from attached distribution list files.	Content Submission		R3 Must
RD-2135	The system shall be able to provide distribution list information to authorized users.	Content Submission		R3 Must
RD-2137	The system shall provide the capability for Service Providers to download distribution list information for jobs that have been awarded to them.	Content Submission		R3 Must
RD-2139	The system shall provide the capability for users to select shipping providers from a configurable list.	Content Submission		R3 Must
RD-2140	The system shall have the capability to provide estimated shipping costs based upon BPI.	Content Submission		R3 Could
RD-2142	The system shall maintain Service Provider information.	Content Submission		R3 Must
RD-2143	Authorized users shall have the capability to access Service Provider information.	Content Submission		R3 Must
RD-2144	The system shall provide the capability for users to create Service Provider information.	Content Submission		R3 Must
RD-2145	The system shall provide the capability for authorized users to edit Service Provider information.	Content Submission		R3 Must
RD-2146	The system shall provide the capability for authorized users to delete Service Provider information.	Content Submission		R3 Must
RD-2147	Service Provider contact information shall include the company name.	Content Submission		R3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2148	The system shall allow users to submit feedback on Service Providers.	Content Submission		R3 Could
RD-2149	Service Provider contact information shall include the physical address.	Content Submission		R3 Must
RD-2150	Service Provider contact information shall include the mailing address.	Content Submission		R3 Must
RD-2151	Service Provider contact information shall include the shipping address.	Content Submission		R3 Must
RD-2152	Service Provider contact information shall include the names of zero or more contact personnel.	Content Submission		R3 Must
RD-2153	Service Provider contact information shall include zero or more phone numbers.	Content Submission		R3 Must
RD-2154	Service Provider contact information shall include zero or more cell phone numbers.	Content Submission		R3 Must
RD-2155	Service Provider contact information shall include zero or more e-mail address.	Content Submission		R3 Must
RD-2156	Service Provider contact information shall include zero or more fax numbers.	Content Submission		R3 Must
RD-2157	Service Provider contact information shall include the state code.	Content Submission		R3 Must
RD-2158	Service Provider contact information shall include the contractor code.	Content Submission		R3 Must
RD-2161	The system shall allow authorized users to manage a list of equipment categories.	Content Submission		R3 Must
RD-2162	Service Providers shall be able to specify the equipment categories they meet from a predefined list.	Content Submission		R3 Must
RD-2163	Service Providers shall be able to manage their equipment categories from a predefined list.	Content Submission		R3 Must
RD-2164	The system shall provide a text field for Service Providers to specify specific equipment they utilize.	Content Submission		R3 Must
RD-2165	Service Providers shall be able to specify products and services that they are capable of providing from a configurable list.	Content Submission		R3 Must
RD-2166	The system shall allow authorized users to manage a configurable list of products and services.	Content Submission		R3 Must
RD-2167	The system shall allow Service Providers to input customized capabilities not included on the configurable list in a note field.	Content Submission		R3 Must
RD-2169	The system shall maintain Service Provider performance information comprised of quality history, quality level, compliance history, and notices.	Content Submission		R3 Must
RD-2170	The system shall allow authorized users to manage Service Provider performance information.	Content Submission		R3 Must
RD-2171	Quality levels shall be assigned by authorized GPO personnel in accordance with GPO Publication 310.1.	Content Submission		R3 Must
RD-2172	Service Provider information shall include quality history data.	Content Submission		R3 Must
RD-2173	Quality history data shall include the number of jobs completed at given quality levels.	Content Submission		R3 Must
RD-2174	Quality history data shall include the number of jobs inspected at given quality level	Content Submission		R3 Must
RD-2175	Quality history data shall include the number of jobs rejected at given quality levels	Content Submission		R3 Must
RD-2176	Service Provider information shall include compliance history data.	Content Submission		R3 Must
RD-2177	Compliance history shall include the number of jobs completed.	Content Submission		R3 Must
RD-2178	Compliance history shall include the number of jobs completed late	Content Submission		R3 Must
RD-2179	Compliance history shall include the percentage of job completed late.	Content Submission		R3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2180	Service Provider information shall include notices.	Content Submission		R3 Must
RD-2181	Notices received shall include the number of cure notices.	Content Submission		R3 Must
RD-2182	Notices received shall include the number of show-cause notices.	Content Submission		R3 Must
RD-2183	Notices received shall include the number of shipped short letters.	Content Submission		R3 Must
RD-2184	Notices received shall include the number of do not condone letters.	Content Submission		R3 Must
RD-2185	Notices received shall include the number of terminations for default (program).	Content Submission		R3 Must
RD-2186	Notices received shall include the number of terminations for default (jobs).	Content Submission		R3 Must
RD-2187	Notices received shall include the number of erroneous information letters.	Content Submission		R3 Must
RD-2188	Notices received shall include the number of non-responsible quality history letters.	Content Submission		R3 Must
RD-2189	Notices received shall include the number of non-responsible performance letters.	Content Submission		R3 Must
RD-2190	Notices received shall include the number of non-responsible other letters.	Content Submission		R3 Must
RD-2191	Notices received shall include the number of exception clause letters	Content Submission		R3 Must
RD-2192	Service Provider information shall include note text field.	Content Submission		R3 Must
RD-2193	The system shall provide the capability to search Service Provider information.	Content Submission		R3 Must
RD-2194	The system shall generate a list of Service Providers in response to a user search request.	Content Submission		R3 Must
RD-2196	The system shall allow authorized users to generate solicitations.	Content Submission		R3 Must
RD-2197	The system shall distribute solicitations.	Content Submission		R3 Must
RD-2198	The system shall accept bids from Service Providers for jobs.	Content Submission		R3 Must
RD-2199	The system shall allow authorized users to submit bid information.	Content Submission		R3 Must
RD-2200	The system shall accept bids with zero to many line items.	Content Submission		R3 Must
RD-2201	The system shall be able to accept bids in the form of a quantity based upon a fixed price (e.g., Service Provider submits quantity of a bid for a fixed dollar amount, How many copies can you print for $100).	Content Submission		R3 Must
RD-2202	The system shall electronically stamp bids with the time it was received.	Content Submission		R3 Must
RD-2203	The system shall electronically stamp bids with the date it was received.	Content Submission		R3 Must
RD-2204	The system shall electronically stamp bids with user profile information.	Content Submission		R3 Must
RD-2205	The system shall allow authorized users to enter electronic stamp information when tangible bids are received.	Content Submission		R3 Must
RD-2206	The system shall allow authorized users to electronically post bid results.	Content Submission		R3 Must
RD-2207	The system shall allow Service Specialists and Content Originators to award jobs to Service Providers.	Content Submission		R3 Must
RD-2210	The system shall allow authorized users to approve contract modifications.	Content Submission		R2 Should /R3 Must
RD-2211	The system shall allow authorized users to manage contract modifications.	Content Submission		R2 Should /R3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2216	Activities include that the job was made available to Service Provider.	Content Submission		R3 Must
RD-2217	Activities include that the job was received by Service Provider.	Content Submission		R3 Must
RD-2218	Activities include that the proofs were sent to Content Originator	Content Submission		R3 Must
RD-2219	Activities include that the proofs were received by Content Originator	Content Submission		R3 Must
RD-2220	Activities include that the proofs were approved.	Content Submission		R3 Must
RD-2221	Activities include that the proofs were approved with author's alterations.	Content Submission		R3 Must
RD-2222	Activities include that the proofs were approved with Service Provider's errors.	Content Submission		R3 Must
RD-2223	Activities include that new proofs were requested due to author's alterations.	Content Submission		R3 Must
RD-2224	Activities include that new proofs were requested due to Service Provider's errors.	Content Submission		R3 Must
RD-2225	Activities include that proofs were sent to Service Provider.	Content Submission		R3 Must
RD-2226	Activities include that proofs were received by Service Provider.	Content Submission		R3 Must
RD-2227	Activities include that changes were made by Content Originator.	Content Submission		R3 Must
RD-2229	Activities include that the job is complete.	Content Submission		R3 Must
RD-2230	Activities include that the job is delivered to each individual destination.	Content Submission		R3 Must
RD-2231	Activities include job shipped to all destinations.	Content Submission		R3 Must
RD-2232	Activities include job delivered to all destinations.	Content Submission		R3 Must
RD-2233	Activities include job delivery receipts are available.	Content Submission		R3 Must
RD-2235	Activities include Job ID referenced,	Content Submission		R3 Must
RD-2236	Activities include approved for publication.	Content Submission		R3 Must
RD-2239	The system shall provide a means to add notes to each job.	Content Submission		R3 Must
RD-2240	The system shall provide the capability to automatically request job status information from users.	Content Submission		R3 Must
RD-2242	The system shall have the capability for authorized users to request automated notifications of job activities.	Content Submission		R3 Must
RD-2243	The system shall allow Service Specialists to generate notifications to Service Providers and Content Originators.	Content Submission		R3 Must
RD-2244	The system shall allow Service Specialists to distribute notification to Service Providers and Content Originators.	Content Submission		R3 Must
RD-2245	Notifications include show cause notices.	Content Submission		R3 Must
RD-2246	Notifications include cure notices.	Content Submission		R3 Must
RD-2247	Notifications include GPO Form 907.	Content Submission		R3 Must
RD-2248	The system shall have the capability to provide shipping notification to authorized users.	Content Submission		R3 Must
RD-2249	The system shall have the capability to provide delivery notification to authorized users.	Content Submission		R3 Must
RD-2250	Notification of delivery shall include tracking numbers from the Service Provider.	Content Submission		R3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2251	Notification of delivery shall include signed delivery receipts.	Content Submission		R3 Must
RD-2252	The system shall have the capability to upload digitized signed delivery receipts.	Content Submission		R3 Must
RD-2253	Notification of delivery shall include confirmation of delivery from agency recipients.	Content Submission		R3 Must
RD-2254	The system shall have the capability to provide users with options in response to undelivered content (e.g., resubmit content, cancel fulfillment).	Content Submission		R2 Should /R3 Must
RD-2256	The system shall have the capability to receive and store product delivery tracking numbers (e.g., Fed-Ex Tracking Number) from Service Providers.	Content Submission		R2 Should /R3 Must
RD-2257	The system shall have the capability to receive confirmation of delivery from the agency or end user.	Content Submission		R2 Should /R3 Must
RD-2258	The system shall have the capability to support Job Definition Format (JDF).	Content Submission		R3 Could
RD-2430	The system shall provide content to delivery processing for the purpose of fulfilling an Content Originator order.	Content Submission		R2 Must
RD-2431	The system shall provide metadata to delivery processing for the purpose of fulfilling an Content Originator order.	Content Submission		R2 Must
RD-2432	The system shall provide business process information to delivery processing for the purpose of fulfilling a Content Originator order.	Content Submission		R2 Must
RD-2877	FDsys shall notify users that content is available for selection for the sales program.	Content Submission		R2 Must
RD-3027	The system must provide a workbench for Content Originators that is based on their user role.	Content Submission		R2 Must
RD-3060	The system shall provide desktop facsimile for GPO Service Specialists to contact users for user assistance.	Content Submission		R2 Could
RD-3260	The system shall support the capability for a user to pull a PIB from the system using additional methods in the future.	Content Submission		R3 Must
RD-3301	The system shall provide the capability for authorized users to define criteria for new notification services.	Content Submission		R2 Must
RD-3310	Users shall have the capability to sign up to receive PIBs by e-mail for new orders they have been awarded.	Content Submission		R2 Must
RD-3313	Users shall have the capability to sign up to receive PIBs by FTP for new orders they have been awarded.	Content Submission		R2 Must
RD-3314	The system shall have the capability to push PIBs to users using Secure File Transfer Protocol.	Content Submission		R3 Must
RD-3315	The system shall support the capability to push PIBs to users using additional methods in the future.	Content Submission		R3 Must
RD-3325	The maximum size PIB delivered by a future electronic channel shall be configurable by an authorized user.	Content Submission		R3 Must
RD-3502	User shall have the capability to post jobs prior to content being approved for ingest.	Content Submission		R3 Must
RD-3503	Users shall have the capability to accept bids prior to content being approved for ingest.	Content Submission		R3 Must
RD-3504	Users shall have the capability to post jobs prior to content being received.	Content Submission		R3 Must
RD-3505	Users shall have the capability to accept bids prior to content being received.	Content Submission		R3 Must
RD-3506	The system shall have the capability to automatically add job tracking information based on workflow events using the job ID.	Content Submission		R3 Must
RD-3587	The system shall provide the capability to edit a job activity list.	Content Submission		R3 Must
RD-3588	The system shall proved the capability to add notes that describe changes to an activity list.	Content Submission		R3 Must
RD-453	The system shall notify users when near duplicate content is detected.	Content Submission		R3 Must

3.5 GPO ACCESS FEATURE GROUP REQUIREMENTS

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2466	FDsys Web-based GUIs shall be Section 508 compliant according to 36 CFR Part 1194.22.	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2467	A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2469	Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2470	Documents shall be organized so they are readable without requiring an associated style sheet.	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2473	Row and column headers shall be identified for data tables.	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2474	Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2475	Frames shall be titled with text that facilitates frame identification and navigation.	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2477	A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2478	When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by assistive technology.	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2479	When a web page requires another application be present on the client system to interpret page content the page shall provide a link to the required tool that complies with 36 CFR1194.21 (a) through (l).	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2489	When electronic forms are designed to be completed on-line, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2490	A method shall be provided that permits users to skip repetitive navigation links.	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2491	When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2963	Public user GUIs shall be section 508 compliant according to 36 CFR Part 1194.21	GPO Access	508 Compliant User Interfaces	R1C2 Must
RD-2994	The system shall provide public user GUIs that allow users to browse content by collection.	GPO Access	Browse Content	R1C2 Must
RD-2995	The system shall provide public user GUIs that allow users to browse by drilling down into content collections based on the natural content boundary of the collection.	GPO Access	Browse Content	R1C2 Must
RD-3800	The system shall provide public user GUIs that allow users to browse content by Government author.	GPO Access	Browse Content	R1C3 Must
RD-3803	The system shall provide a public user GUIs that allow users to browse content by date issued (i.e., publication date).	GPO Access	Browse Content	R1C2 Must
RD-3805	The system shall provide a public user GUIs that allow users to browse content by collection specific metadata elements.	GPO Access	Browse Content	R1C3 Must
RD-3381	The system shall provide the capability for authorized users to manually transform non-section 508 compliant content into section 508 compliant content.	GPO Access	Checking/Reformatting Content for 508 Compliance	R1C3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3793	The system shall record in metadata when a section 508 rendition has been created.	GPO Access	Checking/Reformatting Content for 508 Compliance	R1C3 Must
RD-470	The system shall provide the capability for authorized users to manually assess content for section 508 accessibility compliance.	GPO Access	Checking/Reformatting Content for 508 Compliance	R1C3 Must
RD-2333	The system shall provide the capability to create persistent links to publicly available renditions of publications listed in RD-2596.	GPO Access	Create Persistent Links	R1C2 Must
RD-2339	The system shall provide the capability to create predictable links to publicly available renditions of publications listed in RD-2596.	GPO Access	Create Persistent Links	R1C2 Must
RD-2340	The system shall provide the capability for internal linking of publications listed in RD-2596 (list of GPO Access applications) at all available levels of granularity.	GPO Access	Create Persistent Links	R1C2 Must
RD-2350	The system shall provide the capability to link articles listed in the Federal Register Table of Contents to articles in the corresponding versions of publicly available Federal Register rendition granules.	GPO Access	Create Persistent Links	R1C2 Must
RD-3744	The system shall provide the capability to create persistent links to publicly available granules of renditions of publications listed in RD-2596.	GPO Access	Create Persistent Links	R1C2 Must
RD-3745	The system shall provide the capability to create predictable links to publicly available granules of renditions of publications listed in RD-2596.	GPO Access	Create Persistent Links	R1C2 Must
RD-119	The system shall provide the capability to deliver metadata from a single publication via GUI links.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-120	The system shall provide the capability to deliver packaged DIPS that contain content and metadata from a single publication via GUI links.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-22	The system shall provide the ability to deliver content independently of its digital format.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-2766	The system shall provide the capability for users to request delivery of content.	GPO Access	Deliver Content and/or Metadata	R1C3 Must
RD-2767	The system shall provide the capability for users to request delivery of metadata.	GPO Access	Deliver Content and/or Metadata	R1C3 Must
RD-2770	The system shall provide the capability for End Users to request no-fee content delivery.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-2840	The system shall provide the capability for users to select format from available options prior to delivery.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-2849	The system shall provide the capability for users to select metadata schema or input standards from available supported options.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3249	The system shall have the capability to create DIPs from ACPs based upon a user request.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3252	The system shall have the capability to deliver DIPs.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3330	The system shall provide the capability for users to download content, metadata, and packages from the system via HTTP.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3385	The system shall have the capability to deliver content to a Windows platform.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3386	The system shall have the capability to deliver content to a Macintosh platform.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3395	The system shall have the capability to deliver electronic content in XML that is equivalent to the original file as ingested.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3396	The system shall have the capability to deliver electronic content in HTML with linked files (e.g., JPEG, GIF, MPEG, MP3) referenced in the HTML code that is equivalent to the original file as ingested.	GPO Access	Deliver Content and/or Metadata	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3397	The system shall have the capability to deliver electronic content in XHTML with linked files (e.g., JPEG, GIF, MPEG, MP3) referenced in the XHTML code that is equivalent to the original file as ingested.	GPO Access	Deliver Content and/or Metadata	R1C3 Must
RD-3398	The system shall have the capability to deliver electronic content in text that is equivalent to the original file as ingested.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3406	The system shall have the capability to deliver electronic content in Microsoft Excel (.xls) format that is equivalent to the original file as ingested.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3410	The system shall have the capability to deliver electronic content in PDF that is equivalent to the original file as ingested.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3425	The system shall have the capability to deliver electronic content that maintains desired user functionality to the extent possible.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3427	The system shall deliver electronic content that maintains interactive content functionality to the extent possible.	GPO Access	Deliver Content and/or Metadata	R1C3 Must
RD-3462	The system shall have the capability to deliver DIPs to GPO storage devices.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3465	The system shall have the capability to deliver DIPs to non-GPO storage devices.	GPO Access	Deliver Content and/or Metadata	R1C3 Must
RD-3723	The system shall provide the capability to deliver packaged DIPs that contain content that is stored in the system and metadata expressed in schemas supported by the schema registry.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3724	The system shall provide the capability to format the presentation of metadata from a single publication that is displayed via GUI links.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3725	The system shall provide the capability to deliver content from a single publication via GUI links.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3733	The ACP cache shall only contain public access renditions of final published content and associated metadata.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3734	The system shall provide the capability for authorized users to prevent external ACPs from being created from internal ACPs.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3778	The system shall provide the capability for users to request delivery of packages.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3780	The system shall provide the capability for public users to select delivery of PREMIS via a link on the content detail GUI.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3781	The system shall provide the capability for public users to select delivery of MODS via a link on the content detail GUI.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3782	The system shall provide the capability for public users to select delivery of MARC via a link on the content detail GUI.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3795	The system shall have the capability to deliver electronic content in ZIP format that is equivalent to the original file as ingested.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3849	The system shall have the capability to deliver metadata in any input standard or extension schema in the schema registry regardless of the schema in which it is stored.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-385	A DIP shall provide the capability to contain one or more renditions of one publication.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-386	A DIP shall provide the capability to contain metadata about each rendition it contains.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-387	The system shall copy content and metadata to a DIP from the publication's ACP.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-392	The DIP shall have the capability to contain one publication that may consist of one or more granules.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-393	The DIP shall have the capability to refer to one or more metadata files associated with the content.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-394	The DIP shall have the capability to refer to one or more digital objects associated with metadata.	GPO Access	Deliver Content and/or Metadata	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-405	The system shall have the capability to assemble optimally packaged DIPs based on the content type desired by the user.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-409	A DIP shall provide the capability to contain a METS file named dip.xml.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-420	The DIP shall have the capability to include all information from the copy of the ACP that is stored in the CMS.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-421	The DIP shall have the capability to include all information from copy of the ACP that is stored in the ACP cache.	GPO Access	Deliver Content and/or Metadata	R1C2 Must
RD-3790	The system shall provide the capability for public users to email a link to a publication.	GPO Access	Delivery By Email	R1C2 Must
RD-3256	The system shall provide the capability for DIP delivery to an authorized user via FTP get.	GPO Access	Delivery By Ftp	R1C2 Must
RD-3302	The system shall provide the capability for DIP delivery to an authorized user via FTP put.	GPO Access	Delivery By Ftp	R1C2 Must
RD-329	The system shall provide the capability for an authorized user to manually transform renditions of ACPs.	GPO Access	Format Transformation	R1C2 Must
RD-3546	The system shall support the transformation of PostScript digital objects into PDF digital objects.	GPO Access	Format Transformation	R1C3 Must
RD-3553	The system shall support the transformation of PDF digital objects into PDF digital objects of lower optimization.	GPO Access	Format Transformation	R1C3 Must
RD-3554	The system shall support the transformation of PDF digital objects into PDF digital objects with searchable text.	GPO Access	Format Transformation	R1C3 Must
RD-3841	The system shall create an XML preservation rendition, where possible, of in-scope content upon ingest.	GPO Access	Format Transformation	R1C2 Must
RD-389	The system shall provide the capability to generate screen optimized renditions for inclusion in the DIP.	GPO Access	Format Transformation	R1C3 Must
RD-575	The system shall support the transformation of PDF digital objects into HTML digital objects.	GPO Access	Format Transformation	R1C2 Must
RD-576	The system shall support the transformation of PDF digital objects into ASCII digital objects.	GPO Access	Format Transformation	R1C2 Must
RD-591	The system shall provide an interface to integrate transforming technologies as required.	GPO Access	Format Transformation	R1C2 Must
RD-609	The system shall support the transformation of XML digital objects into other registered XML digital objects.	GPO Access	Format Transformation	R1C2 Must
RD-610	The system shall support the transformation of XML metadata into other registered XML metadata.	GPO Access	Format Transformation	R1C2 Must
RD-611	The system shall support the transformation of system metadata into other registered XML metadata.	GPO Access	Format Transformation	R1C2 Must
RD-612	The system shall have the capability to perform transformations without deleting the content that has been acted upon.	GPO Access	Format Transformation	R1C2 Must
RD-613	The system shall provide the capability to apply quality metrics to format transformations.	GPO Access	Format Transformation	R1C2 Must
RD-699	The system shall provide the capability to deliver PDF access renditions that are identical in formatting to the print rendition, if a print rendition is available.	GPO Access	Format Transformation	R1C2 Must
RD-2331	The system shall provide access to content currently available on GPO Access.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-2771	The system shall not restrict or otherwise diminish access to items that are currently available through GPO Access.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-2773	The system shall maintain printing functionality currently available within GPO Access content collections.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-2774	The system shall maintain downloading functionality currently available within GPO Access content collections.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-3779	The system shall provide the capability to segment content.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-3851	The system shall ingest content currently available on GPO Access.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-3852	The system shall migrate existing GPO Access GUIs by replacing, updating, or providing new functionality.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3853	The system shall have the capability to ingest all day-forward content for collections currently available on GPO Access.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-3857	The system shall provide the capability to ingest MODS files for migrated GPO Access content.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-3858	The system shall interface with the GPO Automated PDF Signing System (APS) for the application of digital signatures on publicly available PDF files.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-3859	The system shall add GPO's digital signature to publicly available PDF files that are delivered to users.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-3860	The system shall include a non-digitally signed rendition of publicly available PDF content in the ACP along with a digitally signed PDF rendition.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-3861	The system shall include a non-digitally signed rendition of PDF content in the AIP.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-3862	The system shall provide access to digitally signed PDF content in public user search results.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-921	When electronic content in PDF format has been authenticated prior to ingest into FDsys (e.g., via the bulk signing tool), the system shall maintain that externally provided authentication.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-922	When electronic content in PDF format has been authenticated prior to ingest into FDsys (e.g., via the bulk signing tool), the system shall deliver the integrity mark to End Users with that externally provided authentication still intact.	GPO Access	Maintain GPO Access Capabilities	R1C2 Must
RD-2581	The system shall provide the capability to ingest PDF files containing "post-it" note comments.	GPO Access	Maintain PDF Features	R1C2 Must
RD-2582	The system shall provide the capability to maintain "post-it" note comments on ingested PDF files as the files are processed through the system.	GPO Access	Maintain PDF Features	R1C2 Must
RD-2583	The system shall provide the capability to maintain PDF features (e.g. bookmarks, comments, links, thumbnails) when PDF files go through a segmentation process.	GPO Access	Maintain PDF Features	R1C2 Must
RD-2584	The system shall provide the capability to maintain PDF features (e.g. bookmarks, comments, links, thumbnails) when PDF files go through a parsing process.	GPO Access	Maintain PDF Features	R1C2 Must
RD-2586	The system shall provide the capability to index content within a PDF "post-it" note comment.	GPO Access	Maintain PDF Features	R1C2 Must
RD-2587	The system shall provide the capability to deliver PDF files that contain "post-it" note comments.	GPO Access	Maintain PDF Features	R1C2 Must
RD-2326	The system shall provide the capability to limit access to content that is out of scope for GPO's dissemination programs.	GPO Access	Manage Public Access	R1C2 Must
RD-2327	The system shall provide the capability to limit access to content that has not been approved by authorized users for public release.	GPO Access	Manage Public Access	R1C2 Must
RD-2328	The system shall provide the capability to limit access to embargoed content until the appropriate release date and time as specified by authorized users.	GPO Access	Manage Public Access	R1C2 Must
RD-2361	The system shall provide the capability for users to access in scope final published versions of ACPs.	GPO Access	Manage Public Access	R1C2 Must
RD-2417	The system shall provide the capability to manage content that is used for access.	GPO Access	Manage Public Access	R1C2 Must
RD-2418	The system shall provide the capability to manage metadata that is used for access.	GPO Access	Manage Public Access	R1C2 Must
RD-2423	The system shall provide the capability for an ACP to be created from an AIP.	GPO Access	Manage Public Access	R1C2 Must
RD-2424	The system shall provide the capability for an existing ACP to be modified.	GPO Access	Manage Public Access	R1C2 Must
RD-279	The system shall provide the capability to prevent an ACP from being created after ingest.	GPO Access	Manage Public Access	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3737	The system shall provide the capability to update metadata in the ACP when metadata in the AIP is changed.	GPO Access	Manage Public Access	R1C2 Must
RD-3738	The system shall provide the capability to add a new rendition to the AIP when content in the ACP is changed.	GPO Access	Manage Public Access	R1C2 Must
RD-3739	The system shall provide the capability to update metadata in the AIP when metadata in the ACP is changed.	GPO Access	Manage Public Access	R1C2 Must
RD-3740	For all publicly available content, the publicly available content shall be the same as the content available to authorized users.	GPO Access	Manage Public Access	R1C2 Must
RD-3741	For all publicly available metadata, the publicly available metadata shall be the same as the metadata available to authorized users.	GPO Access	Manage Public Access	R1C2 Must
RD-3752	The system shall provide the capability to designate metadata elements as mandatory for access.	GPO Access	Manage Public Access	R1C2 Must
RD-639	The system shall provide the capability to update content in the ACP when content is added to the AIP.	GPO Access	Manage Public Access	R1C2 Must
RD-748	The system shall resolve legacy existing GPO naming schemes.	GPO Access	Purl / Getdoc / Getpage / Getcfr Resolution	R1C2 Must
RD-749	The system shall resolve existing PURLs.	GPO Access	Purl / Getdoc / Getpage / Getcfr Resolution	R1C2 Must
RD-750	The system shall resolve existing URLS that were constructed using GetDoc.	GPO Access	Purl / Getdoc / Getpage / Getcfr Resolution	R1C2 Must
RD-751	The system shall resolve existing URLS that were constructed using GetPage.	GPO Access	Purl / Getdoc / Getpage / Getcfr Resolution	R1C2 Must
RD-752	The system shall resolve existing URLS that were constructed using GetCFR.	GPO Access	Purl / Getdoc / Getpage / Getcfr Resolution	R1C2 Must
RD-2556	The system shall provide the capability to search for and retrieve content from the system.	GPO Access	Search	R1C2 Must
RD-2557	The system shall provide the capability to search for and retrieve metadata from the system.	GPO Access	Search	R1C2 Must
RD-2561	The system shall provide the capability to search content that is currently available on the GPO Access public Web site.	GPO Access	Search	R1C2 Must
RD-2563	The system shall provide the capability to search and retrieve unstructured content (e.g., text).	GPO Access	Search	R1C2 Must
RD-2564	The system shall provide the capability to match character strings (e.g., search exact phrases).	GPO Access	Search	R1C2 Must
RD-2565	The system shall provide the capability to search and retrieve semi-structured content (e.g., inline markup).	GPO Access	Search	R1C2 Must
RD-2566	The system shall provide the capability to search and retrieve structured content (e.g., fielded).	GPO Access	Search	R1C2 Must
RD-2567	The system shall provide the capability to search for content by means of querying metadata.	GPO Access	Search	R1C2 Must
RD-2589	The system shall provide the capability for users to select content collections to search.	GPO Access	Search	R1C2 Must
RD-2591	The system shall provide the capability for users to select search complexity levels (e.g., simple search, advanced/fielded search).	GPO Access	Search	R1C2 Must
RD-2592	The system shall provide a simple search that allows users to search across content collections.	GPO Access	Search	R1C2 Must
RD-2593	The system shall provide an advanced/fielded search that allows users to search for specific terms in specific metadata fields.	GPO Access	Search	R1C2 Must
RD-2594	The system shall allow searching on any number of collections of content.	GPO Access	Search	R1C2 Must
RD-2595	The system shall allow users to search any collection based on the metadata associated with that collection.	GPO Access	Search	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2596	The system shall provide access to GPO Access collections.	GPO Access	Search	R1C2 Must
RD-2597	The system shall provide access to the Public and Private Laws collection.	GPO Access	Search	R1C2 Must
RD-2598	The system shall provide access to the Congressional Reports collection including House, Senate, and Senate Executive Reports.	GPO Access	Search	R1C2 Must
RD-2599	The system shall provide access to the Congressional Documents collection including House Documents, Senate Documents, Senate Executive Documents, and Senate Treaty Documents.	GPO Access	Search	R1C2 Must
RD-2600	The system shall provide access to the Congressional Bills collection.	GPO Access	Search	R1C2 Must
RD-2601	The system shall provide access to the Federal Register collection.	GPO Access	Search	R1C2 Must
RD-2602	The system shall provide access to the History of Bills collection.	GPO Access	Search	R1C2 Must
RD-2603	The system shall provide access to the Congressional Record collection.	GPO Access	Search	R1C2 Must
RD-2604	The system shall provide access to the Congressional Record Index collection.	GPO Access	Search	R1C2 Must
RD-2605	The system shall provide access to the United States Code collection including browse, 1994, and 2000.	GPO Access	Search	R1C2 Must
RD-2606	The system shall provide access to the Code of Federal Regulations collection	GPO Access	Search	R1C2 Must
RD-2607	The system shall provide access to the List of Sections Affected (LSA) collection.	GPO Access	Search	R1C2 Must
RD-2608	The system shall provide access to the Congressional Hearings collection including House Appropriations, Senate Appropriations, and Supreme Court Nomination Hearings.	GPO Access	Search	R1C2 Must
RD-2609	The system shall provide access to the Congressional Committee Prints collection.	GPO Access	Search	R1C2 Must
RD-2610	The system shall provide access to the Congressional Calendars collection including House, Senate, and Committee calendars.	GPO Access	Search	R1C2 Must
RD-2611	The system shall provide access to the Weekly Compilation of Presidential Documents collection.	GPO Access	Search	R1C2 Must
RD-2612	The system shall provide access to the Budget of the United States Government collection including the Citizen's Guide to the Federal Budget.	GPO Access	Search	R1C2 Must
RD-2613	The system shall provide access to the Bound Congressional Record collection.	GPO Access	Search	R1C2 Must
RD-2614	The system shall provide access to the House Journal collection.	GPO Access	Search	R1C2 Must
RD-2615	The system shall provide access to the Semiannual Regulatory Agenda (Unified Agenda) collection.	GPO Access	Search	R1C2 Must
RD-2616	The system shall provide access to the U.S. Constitution Analysis and Interpretation collection.	GPO Access	Search	R1C2 Must
RD-2617	The system shall provide access to the Economic Indicators collection.	GPO Access	Search	R1C2 Must
RD-2618	The system shall provide access to the Economic Report of the President collection.	GPO Access	Search	R1C2 Must
RD-2619	The system shall provide access to the Congressional Directory collection.	GPO Access	Search	R1C2 Must
RD-2620	The system shall provide access to the U.S. Government Manual collection.	GPO Access	Search	R1C2 Must
RD-2621	The system shall provide access to the Public Papers of the President of the United States collection.	GPO Access	Search	R1C2 Must
RD-2622	The system shall provide access to the House Ways and Means Committee Prints collection.	GPO Access	Search	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2623	The system shall provide access to the GAO Comptroller General Decisions collection.	GPO Access	Search	R1C2 Must
RD-2624	The system shall provide access to the GAO Reports collection.	GPO Access	Search	R1C2 Must
RD-2625	The system shall provide access to the House Practice collection.	GPO Access	Search	R1C2 Must
RD-2626	The system shall provide access to the Senate Manual collection.	GPO Access	Search	R1C2 Must
RD-2627	The system shall provide access to the House Rules and Manual collection.	GPO Access	Search	R1C2 Must
RD-2628	The system shall provide access to the Privacy Act Issuances collection.	GPO Access	Search	R1C2 Must
RD-2630	The system shall provide access to the U.S. Government Printing Office Style Manual collection.	GPO Access	Search	R1C2 Must
RD-2633	The system shall provide access to the Independent Counsel Investigation Reports.	GPO Access	Search	R1C2 Must
RD-2634	The system shall provide access to the Government Information Locator Service Records (GILS) collection.	GPO Access	Search	R1C2 Must
RD-2636	The system shall provide access to the Davis-Bacon Wage Determinations collection.	GPO Access	Search	R1C2 Must
RD-2637	The system shall provide access to the Commerce Business Daily collection.	GPO Access	Search	R1C2 Must
RD-2638	The system shall provide access to the Congressional Publications collection.	GPO Access	Search	R1C2 Must
RD-2639	The system shall provide access to the Statutes at Large collection.	GPO Access	Search	R1C2 Must
RD-2642	The system shall provide access to the Background Material and Data on Programs within the Jurisdiction of the Committee on Ways and Means (Green Book) collection.	GPO Access	Search	R1C2 Must
RD-2643	The system shall provide access to the Conference Reports collection.	GPO Access	Search	R1C2 Must
RD-2644	The system shall provide access to the Education Reports from ERIC collection.	GPO Access	Search	R1C2 Must
RD-2647	The system shall provide access to the Riddick's Senate Procedures collection.	GPO Access	Search	R1C2 Must
RD-2648	The system shall provide access to the United States Government Policy and Support Positions (Plum Book) collection.	GPO Access	Search	R1C2 Must
RD-2655	The system shall provide access to the Export Administration Regulations collection.	GPO Access	Search	R1C2 Must
RD-2657	The system shall provide access to the State of Union Addresses collection.	GPO Access	Search	R1C2 Must
RD-2665	The system shall provide access to the Supreme Court Decisions 1937-1975 collection.	GPO Access	Search	R1C2 Must
RD-2669	The system shall provide access to the Congressional Serial Set superset collection.	GPO Access	Search	R1C2 Must
RD-2670	The system shall provide access to the Congressional Committee Materials superset collection.	GPO Access	Search	R1C2 Must
RD-2682	The system shall support standard Boolean search language.	GPO Access	Search	R1C2 Must
RD-2683	The system shall support full Boolean operators, including AND, OR, NOT.	GPO Access	Search	R1C2 Must
RD-2684	The system shall support implied Boolean operators, including “+” and “-“.	GPO Access	Search	R1C2 Must
RD-2685	The system shall support the nesting of Boolean operators via parentheses.	GPO Access	Search	R1C2 Must
RD-2686	No user shall be required to enter case sensitive operators.	GPO Access	Search	R1C2 Must
RD-2688	The system shall support a editable list of stop words.	GPO Access	Search	R1C3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2689	The system shall support an editable list of idioms.	GPO Access	Search	R1C3 Must
RD-2692	The system shall allow for right side stemming.	GPO Access	Search	R1C2 Must
RD-2693	The system shall allow users to use wildcard characters to replace characters within words.	GPO Access	Search	R1C2 Must
RD-2694	The system shall support proximity searching.	GPO Access	Search	R1C2 Must
RD-2695	The system shall support synonyms searching.	GPO Access	Search	R1C2 Must
RD-2703	The system shall provide the capability for authorized users to limit search query length.	GPO Access	Search	R1C3 Must
RD-2704	The system shall provide the capability to qualify search terms.	GPO Access	Search	R1C2 Must
RD-2706	The system shall provide the capability for users to modify previous search queries to enable execution of subsequent searches.	GPO Access	Search	R1C2 Must
RD-2707	The system shall provide the capability to direct subsequent queries against different content collections.	GPO Access	Search	R1C2 Must
RD-2711	The system shall be able to recognize alternate spellings of search terms.	GPO Access	Search	R1C2 Must
RD-2712	The system shall suggest corrected spellings of search terms.	GPO Access	Search	R1C2 Must
RD-2758	The system design and architecture shall not limit GPO's ability to add new collections.	GPO Access	Search	R1C2 Must
RD-2759	The system shall provide authorized users with access to a Web-based search administrator graphical user interface (GUI).	GPO Access	Search	R1C2 Must
RD-2762	The system shall provide the capability to support user search while other system functions are being performed (e.g., re-indexing databases, updating content).	GPO Access	Search	R1C2 Must
RD-2763	The system shall provide the capability to log search activities.	GPO Access	Search	R1C2 Must
RD-3753	The system shall provide the capability for users to search metadata only.	GPO Access	Search	R1C2 Must
RD-3754	The system shall provide the capability for users to search content only.	GPO Access	Search	R1C2 Must
RD-3755	The system shall provide the capability for users to search content and metadata together.	GPO Access	Search	R1C2 Must
RD-3756	The system shall provide the capability for users to search for granules.	GPO Access	Search	R1C2 Must
RD-3757	The system shall provide the capability to parse metadata elements from content.	GPO Access	Search	R1C2 Must
RD-3758	The system shall provide the capability for users to search by metadata fields available in MODS.	GPO Access	Search	R1C2 Must
RD-3761	The system shall provide the capability to search for content by means of querying metadata for the purpose of retrieving entire publications.	GPO Access	Search	R1C2 Must
RD-3762	The system shall provide the capability to search for content by means of querying metadata for the purpose of retrieving individual granules.	GPO Access	Search	R1C2 Must
RD-3763	The system shall provide access to the Precedents of the House of Representatives collection including Deschler's Cannon's, and Hinds' precedents.	GPO Access	Search	R1C2 Must
RD-3764	The system shall provide access to the Congressional Pictorial Directory collection.	GPO Access	Search	R1C2 Must
RD-3765	The system shall provide access to the Agency Publications collection.	GPO Access	Search	R1C2 Must
RD-3766	The system shall provide access to the Judicial Publications collection.	GPO Access	Search	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3767	The system shall provide access to the New Member Pictorial Directories collection.	GPO Access	Search	R1C2 Must
RD-3768	The system shall support the Boolean operators BEFORE, NEAR, and ADJACENT.	GPO Access	Search	R1C2 Must
RD-3776	The system shall provide authorized users with access to a Web-based search business manager graphical user interface (GUI).	GPO Access	Search	R1C2 Must
RD-3777	The system shall provide the capability for internet search engines to index publicly available content.	GPO Access	Search	R1C2 Must
RD-2717	The system shall provide search results to users.	GPO Access	Search Results	R1C2 Must
RD-2718	The system shall provide the capability to group renditions into one entry in the search results list.	GPO Access	Search Results	R1C2 Must
RD-2719	The system shall allow users to sort search results bi-directionally based on displayable attributes in the result set.	GPO Access	Search Results	R1C2 Must
RD-2725	The system shall provide the capability for users to limit the number of results displayed.	GPO Access	Search Results	R1C2 Must
RD-2726	The system shall provide the capability to display the total number of results in the result set returned by the search.	GPO Access	Search Results	R1C3 Must
RD-2729	The system shall provide the capability for authorized users to select which metadata attributes are viewable in the content detail on a per collection basis.	GPO Access	Search Results	R1C2 Must
RD-2735	The system shall provide feedback to the user in the event of an error.	GPO Access	Search Results	R1C2 Must
RD-2738	The system shall provide the capability to return search results at the lowest level of granularity supported by the content package.	GPO Access	Search Results	R1C2 Must
RD-2740	The system shall provide the capability for users to filter search results.	GPO Access	Search Results	R1C2 Must
RD-2741	The system shall provide the capability for users to return to their original search results after results have been filtered.	GPO Access	Search Results	R1C2 Must
RD-2755	The system shall provide the capability to have navigational elements to allow users to navigate through search results.	GPO Access	Search Results	R1C2 Must
RD-3771	The system shall provide the capability for an authorized user to configure the elements displayed in a search result on a per collection basis.	GPO Access	Search Results	R1C2 Must
RD-3773	The system shall provide the capability to display a document summary in a search result.	GPO Access	Search Results	R1C2 Must
RD-3775	The system shall provide the capability to search within search results.	GPO Access	Search Results	R1C2 Must
RD-3796	The system shall display collection specific search filters after a user has initially selected a collection filter.	GPO Access	Search Results	R1C2 Must
RD-3797	The system shall display collection specific search filters when search results are limited to one collection.	GPO Access	Search Results	R1C2 Must
RD-3798	The system shall provide for the uniform display of search filters.	GPO Access	Search Results	R1C2 Must
RD-2275	The system shall enforce the continuity of content in context.	GPO Access	Support Granularity	R1C2 Must
RD-2332	The system shall provide the capability for users to access select publications enumerated in RD-2596 at a level of granularity that is less than a publication.	GPO Access	Support Granularity	R1C2 Must
RD-2853	The system shall provide the capability for users to select level of granularity from available options.	GPO Access	Support Granularity	R1C2 Must
RD-3787	The system shall provide the capability for users to navigate level of granularity for a publication from available options.	GPO Access	Support Granularity	R1C2 Must
RD-662	The system shall allow GPO to define the level of granularity that content can be retrieved at.	GPO Access	Support Granularity	R1C2 Must
RD-666	The system shall support granularity to the level of a publication.	GPO Access	Support Granularity	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-685	The system shall provide the capability to support granularity down to the lowest level of granularity that maintains context based on natural content boundaries of the publication.	GPO Access	Support Granularity	R1C2 Must
RD-687	The system shall provide the capability to display granular content in search results.	GPO Access	Support Granularity	R1C2 Must
RD-689	The system shall provide the capability to associate granular content in the content detail with the entire publication.	GPO Access	Support Granularity	R1C2 Must
RD-690	The system shall provide the capability to deliver granular content separate from the entire publication.	GPO Access	Support Granularity	R1C2 Must
RD-692	The system shall provide the capability to deliver text-based granular content in a PDF format that has been optimized for rapid access and delivery.	GPO Access	Support Granularity	R1C2 Must
RD-693	The system shall provide the capability to deliver text-based granular content in a HTML format that has been optimized for rapid access and delivery.	GPO Access	Support Granularity	R1C2 Must
RD-694	The system shall provide the capability to deliver text-based granular content in a text format that has been optimized for rapid access and delivery.	GPO Access	Support Granularity	R1C2 Must
RD-695	The system shall provide the capability to deliver text-based granular content in a XML format that has been optimized for rapid access and delivery.	GPO Access	Support Granularity	R1C3 Must
RD-697	The system shall provide the capability to deliver PDF granules at a page level of granularity.	GPO Access	Support Granularity	R1C2 Must
RD-698	The system shall provide the capability to deliver PDF granules at a page range level of granularity if the granules span multiple pages.	GPO Access	Support Granularity	R1C2 Must
RD-3047	The system shall provide web form for users to contact authorized users for user assistance.	GPO Access	User Help	R1C2 Must
RD-3073	The system shall provide context specific help menus that contain user support information related to what is on the current user interface.	GPO Access	User Help	R1C2 Must
RD-3074	The system shall provide context specific help menus that provide access to all available user support information for the system.	GPO Access	User Help	R1C2 Must
RD-3075	The system shall provide the capability for authorized uses to manage information (text, images, audio, video, multimedia) in the context specific help menus.	GPO Access	User Help	R1C2 Must
RD-3078	The system shall provide the capability for user to navigate the context specific help menus using an index.	GPO Access	User Help	R1C2 Must
RD-3079	The system shall provide the capability to have context specific help that consists of descriptive text thats displayed when a user points the mouse over an item on the user interface.	GPO Access	User Help	R1C3 Must
RD-3080	The system shall provide the capability for authorized users to manage descriptive text that is displayed in context specific help when a user points the mouse over an item on the user interface.	GPO Access	User Help	R1C3 Must
RD-3081	The system shall provide the capability to have context specific help that consists of clickable help icons or text on the user interface.	GPO Access	User Help	R1C2 Must
RD-2716	The system shall provide the capability for public users to bookmark search results.	GPO Access	User Interface	R1C2 Must
RD-2824	The system shall provide the capability to display lists of publications as specified by GPO.	GPO Access	User Interface	R1C3 Must
RD-2961	The system shall provide public user GUIs that allows users to access the system without registering.	GPO Access	User Interface	R1C2 Must
RD-2969	The system shall support web-based public user GUIs.	GPO Access	User Interface	R1C2 Must
RD-2983	The system shall provide GUIs that are fully functional in Mozilla Firefox 1.5.x on Macintosh, Windows, and Linux.	GPO Access	User Interface	R1C3 Should

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2984	The system shall provide GUIs that are fully functional in Microsoft Internet Explorer 6.x on Windows.	GPO Access	User Interface	R1C2 Must
RD-2985	The system shall provide GUIs that are fully functional in Mozilla Firefox 2.0.x on Macintosh, Linux, and Windows.	GPO Access	User Interface	R1C2 Must
RD-2986	The system shall provide GUIs that are fully functional in Microsoft Internet Explorer 7.x. on Windows.	GPO Access	User Interface	R1C3 Should
RD-2987	The system shall provide GUIs that are fully functional in Netscape Navigator 7.x on Windows.	GPO Access	User Interface	R1C3 Should
RD-2988	The system shall provide GUIs that are fully functional in Safari 2.x on Macintosh.	GPO Access	User Interface	R1C3 Must
RD-2989	The system shall provide GUIs that are fully functional in Konqueror 2.x on Linux.	GPO Access	User Interface	R1C3 Should
RD-2990	The system shall provide Web pages that are designed based on Web standards.	GPO Access	User Interface	R1C2 Must
RD-2991	The system shall provide static Web pages that are designed using templates.	GPO Access	User Interface	R1C2 Must
RD-2993	The system shall provide GUIs that are capable of providing context specific help and user support.	GPO Access	User Interface	R1C2 Must
RD-3001	The system shall support Extensible Markup Language (XML).	GPO Access	User Interface	R1C2 Must
RD-3002	The system shall support Extensible Style sheet Language (XSL).	GPO Access	User Interface	R1C2 Must
RD-3004	The system shall support Document Type Definition (DTD).	GPO Access	User Interface	R1C2 Must
RD-3005	The system shall support schema.	GPO Access	User Interface	R1C2 Must
RD-3006	The system shall support XSL Transformations (XSLT).	GPO Access	User Interface	R1C2 Must
RD-3007	The system shall support XML Path Language (XPath).	GPO Access	User Interface	R1C2 Must
RD-3008	The system shall support Extensible HyperText Markup Language (XHTML).	GPO Access	User Interface	R1C2 Must
RD-3009	The system shall support Cascading Style Sheets (CSS)	GPO Access	User Interface	R1C2 Must
RD-3010	The system shall support DHTML.	GPO Access	User Interface	R1C2 Must
RD-3054	The system shall provide users with information on how to contact GPO for assistance.	GPO Access	User Interface	R1C2 Must
RD-3769	The system shall provide the capability for public users to bookmark the content detail page.	GPO Access	User Interface	R1C2 Must
RD-3770	The system shall provide the capability for public users to bookmark individual collection pages.	GPO Access	User Interface	R1C2 Must
RD-3788	The system shall maintain a consistent look and feel throughout public user GUIs.	GPO Access	User Interface	R1C2 Must
RD-3789	Public user GUIs shall conform to GPO design guidelines as referenced in FDsys design guidelines.	GPO Access	User Interface	R1C2 Must
RD-3801	The system shall provide public GUIs that display Congressional committee publications associated with each committee.	GPO Access	User Interface	R1C2 Must
RD-3802	The system shall provide public user GUIs for individual GPO Access collections.	GPO Access	User Interface	R1C2 Must
RD-3806	The system shall provide public user GUIs that allow users to learn about Government publications.	GPO Access	User Interface	R1C2 Must
RD-3807	The system shall provide a public user GUI that allow users to receive context specific help in accessing Government publications.	GPO Access	User Interface	R1C2 Must
RD-3808	The system shall provide a public user GUI that allows users to contact GPO for assistance.	GPO Access	User Interface	R1C2 Must
RD-3809	The system shall provide public user content detail GUIs.	GPO Access	User Interface	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3811	The system shall provide a public user FDsys homepage GUI.	GPO Access	User Interface	R1C2 Must
RD-3812	The system shall provide public user search GUIs that enable required search functionality.	GPO Access	User Interface	R1C2 Must
RD-3813	The system shall provide public user search results GUIs.	GPO Access	User Interface	R1C2 Must
RD-3817	The system shall provide 1C GUIs as specified in 1C GUI specifications.	GPO Access	User Interface	R1C2 Must
RD-3842	The system shall provide the capability for authorized users to manage static content in editable area of Web-based GUIs via an HTML editor.	GPO Access	User Interface	R1C2 Must
RD-3843	The system shall provide the capability for authorized users to manage editable areas of CSS style sheets for Web-based GUIs via an HTML editor.	GPO Access	User Interface	R1C2 Must
RD-3844	The system shall provide the capability for authorized users to manage references to images in editable areas on Web-based GUIs via an HTML editor.	GPO Access	User Interface	R1C2 Must
RD-3845	The system shall provide the capability for authorized users to manage hyperlinks in editable area on Web-based GUIs via an HTML editor.	GPO Access	User Interface	R1C2 Must
RD-3846	The system shall provide the capability for authorized users to add static content to editable areas of dynamically generated pages.	GPO Access	User Interface	R1C2 Must
RD-3850	The system shall provide the capability to apply formatting to XML files when they are displayed in a browser.	GPO Access	User Interface	R1C2 Must
RD-3819	The system shall provide the capability to email the daily Federal Register Table of Contents as HTML with content links enabled.	GPO Access	User Notification	R1C2 Must
RD-3820	The system shall provide the capability to email the daily Federal Register Table of Contents as an HTML attachment with content links enabled.	GPO Access	User Notification	R1C2 Must
RD-3821	The system shall provide the capability to email the daily Federal Register Table of Contents as text.	GPO Access	User Notification	R1C2 Must
RD-3822	The system shall provide the capability for public users to sign up to receive the daily Federal Register Table of Contents.	GPO Access	User Notification	R1C2 Must

3.6 INFRASTRUCTURE FEATURE GROUP REQUIREMENTS

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1381	The system shall have the capability to authenticate authorized users based on a unique user identity.	Infrastructure	Authenticate User	R1C2 Must
RD-1385	The system shall support user ID and password authentication.	Infrastructure	Authenticate User	R1C2 Must
RD-1508	System security policy parameters shall include the capability to support various authentication methods.	Infrastructure	Authenticate User	R1C2 Must
RD-1509	System security policy parameters shall include authorized user authentication methods.	Infrastructure	Authenticate User	R1C2 Must
RD-1510	System security policy parameters shall include administrator authentication methods.	Infrastructure	Authenticate User	R1C4 Must
RD-789	The system shall verify the identity and authority of authorized users.	Infrastructure	Authenticate User	R1C2 Must
RD-790	Valid proof of the user's identity shall be logged by the system.	Infrastructure	Authenticate User	R1C2 Must
RD-797	The system shall verify that the content sender is, in fact, the party who claimed to have submitted the content.	Infrastructure	Authenticate User	R1C2 Must
RD-798	The system shall verify that the content recipient is, in fact, the party who claimed to have received the content.	Infrastructure	Authenticate User	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-822	The system shall record the sender and recipient information in metadata.	Infrastructure	Authenticate User	R1C2 Must
RD-823	The system shall verify that the sender is, in fact, the party who claimed to have sent the converted content.	Infrastructure	Authenticate User	R1C4 Must
RD-824	The system shall verify that the recipient is, in fact, the party who claimed to have received the converted content.	Infrastructure	Authenticate User	R1C4 Must
RD-1241	The system shall provide the capability to switchover operations from the primary to the backup site in the event of a disaster.	Infrastructure	COOP	R1C2 Must
RD-1265	Long-term Permanent Archival Storage shall have a remote storage site over 600 miles from the main GPO facility.	Infrastructure	COOP	R1C2 Must
RD-1266	Long-term Permanent Archival Storage site shall preserve physical data integrity and quality for no less than 100 Years under controlled storage conditions (e.g., 70º F, 60% Humidity).	Infrastructure	COOP	R3 Must
RD-1309	BPI shall contain Failover Storage.	Infrastructure	COOP	R1C3 Must
RD-1525	The system shall provide appropriate redundant components to ensure availability to meet customer and GPO needs.	Infrastructure	COOP	R1C2 Must
RD-1526	The system shall be operational in the event of disaster situations with minimal business interruption to business functions.	Infrastructure	COOP	R1C4 Must
RD-1527	The system shall have the capability to return to normal operations post-disaster.	Infrastructure	COOP	R1C2 Must
RD-1528	The system shall adhere to GPO's Continuity of Operations (COOP) plans.	Infrastructure	COOP	R1C4 Must
RD-1529	The system shall adhere to system development guidelines set forth in Office of Management and Budget Circular A-130.	Infrastructure	COOP	R1C2 Must
RD-1530	The system shall adhere to guidelines set forth in Federal Preparedness Circular 65.	Infrastructure	COOP	R1C2 Must
RD-1531	The system shall have appropriate failover components.	Infrastructure	COOP	R1C2 Must
RD-1532	The system shall be operational at appropriate GPO alternate facilities.	Infrastructure	COOP	R1C2 Must
RD-1660	The system shall be capable of extracting data from the entire collection of BPI.	Infrastructure	Data Mining	R2 Must
RD-1661	The system shall be capable of extracting data from the entire collection of metadata.	Infrastructure	Data Mining	R2 Must
RD-1662	The system shall be capable of extracting data from select GPO data sources (e.g., Oracle Financials).	Infrastructure	Data Mining	R3 Must
RD-1663	The system shall be capable of extracting data from Oracle Financials.	Infrastructure	Data Mining	R3 Must
RD-1664	The system shall be capable of extracting data from additional GPO data sources in the future.	Infrastructure	Data Mining	R3 Must
RD-1665	The system shall be capable of extracting data according to a schedule defined by authorized users.	Infrastructure	Data Mining	R1C4 Should / R2 Must
RD-1666	The system shall be able to extract data according to authorized user defined queries.	Infrastructure	Data Mining	R2 Must
RD-1667	The system shall be able to extract random samples of data.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1668	The system shall allow authorized users to input data to supplement system data (e.g., Web log, historical sales data).	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1669	The system shall allow authorized users to upload files from which data will be extracted for analysis.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1670	The system shall allow authorized users to enter supplemental historical data.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1671	The system shall allow authorized users to restrict access to supplemental data.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1672	The system shall allow authorized users to store supplemental data for future use.	Infrastructure	Data Mining	R1C3 Should / R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1673	The system shall be capable of extracting data from multiple formats.	Infrastructure	Data Mining	R2 Must
RD-1674	The system shall be capable of extracting data from data sources in XML format.	Infrastructure	Data Mining	R2 Must
RD-1675	The system shall be capable of extracting data from data sources in PDF format.	Infrastructure	Data Mining	R2 Must
RD-1676	The system shall be capable of extracting data from data sources in XLS format.	Infrastructure	Data Mining	R2 Must
RD-1677	The system shall be capable of extracting data from data sources in CSV format.	Infrastructure	Data Mining	R2 Must
RD-1678	The system shall be support the capability of extracting data from data sources in additional formats in the future.	Infrastructure	Data Mining	R3 Must
RD-1679	The system shall be capable of data extraction at speeds sufficient to support the creation of real-time reports.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1681	The system shall be able to normalize data based on additional administrator defined parameters in the future.	Infrastructure	Data Mining	R2 Must
RD-1682	The system shall be able to identify missing values or metadata elements.	Infrastructure	Data Mining	R2 Must
RD-1683	The system shall be able to identify data anomalies in BPI and metadata.	Infrastructure	Data Mining	R2 Must
RD-1684	The system shall be able to identify data formats.	Infrastructure	Data Mining	R2 Must
RD-1685	The system shall be able to identify format discrepancies.	Infrastructure	Data Mining	R2 Must
RD-1686	The system shall be able to identify standard data elements.	Infrastructure	Data Mining	R2 Must
RD-1687	The system shall be able to identify data types.	Infrastructure	Data Mining	R2 Must
RD-1688	The system shall be able to merge and separate data sets based on administrator defined parameters (e.g., joining or separating fields, removing NULL values, string conversion of date data).	Infrastructure	Data Mining	R2 Must
RD-1690	The system shall be able to perform single variable and multivariable analysis operations on extracted data.	Infrastructure	Data Mining	R2 Must
RD-1691	The system shall be able to perform single variable analysis operations on extracted data.	Infrastructure	Data Mining	R2 Must
RD-1692	The system shall be able to perform multivariable analysis operations on extracted data.	Infrastructure	Data Mining	R2 Must
RD-1693	The system shall be able to calculate averages (mean, median, mode).	Infrastructure	Data Mining	R2 Must
RD-1694	The system shall be able to calculate means.	Infrastructure	Data Mining	R2 Must
RD-1695	The system shall be able to calculate medians.	Infrastructure	Data Mining	R2 Must
RD-1696	The system shall be able to calculate modes.	Infrastructure	Data Mining	R2 Must
RD-1697	The system shall be able to perform cross tabulations.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1698	The system shall be able to perform clusterization.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1699	The system shall be able to perform categorization.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1700	The system shall be able to perform association and link analyses.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1701	The system shall be able to perform regression analysis.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1702	The system shall be able to expose hierarchical or parent/child relationships.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1704	The system shall be able to expose sequential relationships.	Infrastructure	Data Mining	R1C3 Could / R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1705	The system shall be able to expose sequential patterns.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1707	The system shall be able to expose temporal relationships.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1708	The system shall be able to expose temporal patterns.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1709	The system shall be able to expose inferences and rules that led to a result set.	Infrastructure	Data Mining	R2 Could / R3 Must
RD-1710	The system shall be able to warn authorized users attempting illogical operations (e.g., calculating averages out of categorical data).	Infrastructure	Data Mining	R2 Could / R3 Must
RD-1711	The system shall be capable of showing the authorized user the rule violation that led to the warning.	Infrastructure	Data Mining	R2 Could / R3 Must
RD-1713	The system shall allow authorized users to suspend an analysis that is in progress.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1714	The system shall allow authorized users to resume a suspended analysis.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1715	The system shall allow authorized users to restart an analysis from the beginning.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1716	The system shall be capable of providing the authorized user with an estimated analysis time.	Infrastructure	Data Mining	R2 Could / R3 Must
RD-1718	The system shall be able to produce reports summarizing the analysis of BPI and metadata.	Infrastructure	Data Mining	R2 Must
RD-1719	The system shall allow authorized users to choose from the data types available in BPI and metadata and choose operations performed on that data.	Infrastructure	Data Mining	R2 Must
RD-1720	The system shall be able to produce a report summarizing system usage for an authorized user-defined time range.	Infrastructure	Data Mining	R2 Must
RD-1721	The system shall be able to produce a report analyzing the usage of search terms.	Infrastructure	Data Mining	R2 Must
RD-1723	The system shall be capable of including charts in reports.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1724	The system shall be capable of including tables in reports.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1725	The system shall be capable of including graphs in reports.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1726	The system shall allow a set of default report templates to be accessible for each user class.	Infrastructure	Data Mining	R2 Must
RD-1727	The system shall allow authorized users to manage the default templates.	Infrastructure	Data Mining	R2 Must
RD-1728	The system shall allow authorized users to create custom reports and report templates based on access rights to BPI and metadata.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1729	The system shall allow authorized users to create custom report templates.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1730	The system shall allow authorized users to update custom report templates.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1731	The system shall allow authorized users to delete custom report templates.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1732	The system shall be capable of real-time population of report templates.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1733	The system shall be capable of automatically creating reports using report templates according to a schedule defined by authorized users.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1734	The system shall allow authorized users to request notification that a scheduled report is available.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1735	The system shall enable GPO authorized users to restrict view/modify access to customized report templates.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1736	The system shall enable GPO authorized users to control which users can view a report template.	Infrastructure	Data Mining	R1C3 Could / R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1737	The system shall enable GPO authorized users to control which users can modify a report template.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1738	The system shall be capable of delivering reports to authorized users.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1739	The system shall allow authorized users to specify delivery method (e.g., e-mail, RSS, FTP).	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1740	The system shall support the capability to deliver reports to authorized users using E-mail.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1741	The system shall support the capability to deliver reports to authorized users using RSS.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1742	The system shall support the capability to deliver reports to authorized users using FTP.	Infrastructure	Data Mining	R1C3 Could / R2 Must
RD-1743	The system shall be capable of supporting dynamically changing reporting.	Infrastructure	Data Mining	R1C3 Should / R3 Must
RD-1744	The system shall allow authorized users to create notifications based on real-time analysis of BPI or metadata.	Infrastructure	Data Mining	R1C3 Should / R2 Must
RD-1745	The system shall be able to link analysis results to data.	Infrastructure	Data Mining	R2 Could / R3 Must
RD-1746	The system shall be able to expose analysis criteria and algorithms.	Infrastructure	Data Mining	R2 Could / R3 Must
RD-1747	The system shall be able to export results in a format specified by the authorized user (e.g., HTML, MS Word, MS Excel, character-delimited text file, XML, PDF)	Infrastructure	Data Mining	R2 Must
RD-1748	The system shall be able to export reports in HTML format.	Infrastructure	Data Mining	R2 Must
RD-1749	The system shall support customization and personalization functions as defined in the FDsys access, search, request, interface, cataloging and reference tools, and user support requirements.	Infrastructure	Data Mining	R2 Must
RD-1750	The system shall support user interface customization and personalization based on the interactions of a user with the system.	Infrastructure	Data Mining	R2 Must
RD-1751	The system shall support user interface customization by aggregating the interactions of many users with the system.	Infrastructure	Data Mining	R2 Must
RD-1753	The system shall restrict access to extracted data based on user groups.	Infrastructure	Data Mining	R2 Must
RD-1754	The system shall allow authorized users to extract data from security audit logs for data mining	Infrastructure	Data Mining	R2 Must
RD-1767	The system shall manage logs.	Infrastructure	Data Mining	R2 Must
RD-1769	The system shall store extracted data.	Infrastructure	Data Mining	R2 Must
RD-1770	Extracted data shall be held in temporary storage. Once analysis is complete, extracted data is deleted from temporary storage.	Infrastructure	Data Mining	R2 Must
RD-1771	The system shall provide the capability to store the corpus of extracted data.	Infrastructure	Data Mining	R2 Must
RD-1772	The system shall provide the capability to delete selected portions of the corpus of extracted data.	Infrastructure	Data Mining	R2 Must
RD-1773	The system shall provide the capability to reload selected portions of the corpus of extracted data by re-extracting the data.	Infrastructure	Data Mining	R2 Must
RD-1774	The system shall store metadata, supplemental data, reports, report templates, analysis criteria, and algorithms in Business Process Storage.	Infrastructure	Data Mining	R2 Must
RD-1775	The system shall store metadata in Business Process Storage.	Infrastructure	Data Mining	R2 Must
RD-1776	The system shall store supplemental data in Business Process Storage.	Infrastructure	Data Mining	R2 Must
RD-1777	The system shall store reports in Business Process Storage.	Infrastructure	Data Mining	R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1778	The system shall store report templates in Business Process Storage.	Infrastructure	Data Mining	R2 Must
RD-1779	The system shall store analysis criteria in Business Process Storage.	Infrastructure	Data Mining	R2 Must
RD-1780	The system shall store algorithms in Business Process Storage.	Infrastructure	Data Mining	R2 Must
RD-3604	The system shall maintain current reporting functionality.	Infrastructure	Data Mining	R1C2 Must
RD-1578	The system shall provide the capability to interoperate with services or applications deployed in different hardware and software platforms, using industry-accepted standards.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1579	The ESB shall support interoperability with Java Enterprise Edition (JEE).	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1580	The ESB shall support interoperability with .Net.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1581	The ESB shall support interoperability with Web Services.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1582	The ESB shall support interoperability with Java Message Service (JMS).	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1584	The ESB shall support Microsoft Windows Server 2003.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1585	The ESB shall support Red Hat Enterprise Advanced Server 2.1.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1586	The ESB shall support application programmer interfaces in common programming languages.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1587	The ESB shall support application programmer interfaces in C.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1588	The ESB shall support application programmer interfaces in C++.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1589	The ESB shall support application programmer interfaces in Java.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1590	The ESB shall support application programmer interfaces in C#.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1591	The system shall support the ability to authenticate applications and services and control which applications can invoke a service.	Infrastructure	Enterprise Service Bus	R2 Must
RD-1592	The system shall support the capability to authenticate internal processes attempting to invoke a service provided by the system.	Infrastructure	Enterprise Service Bus	R2 Must
RD-1593	The system shall support the capability to authenticate external processes attempting to invoke a service provided by the system.	Infrastructure	Enterprise Service Bus	R2 Must
RD-1594	The system shall provide the capability to integrate newly developed (or acquired) services or applications (e.g. ILS, Oracle Financials) using industry standard protocols.	Infrastructure	Enterprise Service Bus	R1C4 Must
RD-1595	The system shall integrate with Oracle Financials applications and services.	Infrastructure	Enterprise Service Bus	R3 Must
RD-1596	The system shall provide the capability to integrate existing (or legacy) services or applications.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1597	The system shall provide the capability to integrate with the ILS.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1598	The system shall provide the capability to coordinate and manage services or applications in the form of enterprise business processes.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1600	The system shall provide the capability to support synchronous communications between services or applications.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1601	The system shall provide the capability to support asynchronous communications between services or applications.	Infrastructure	Enterprise Service Bus	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1602	The system shall provide the capability to support reliable communications between services or applications.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1603	The system shall provide the capability to specify the quality of service for communications between services or applications.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1604	The system shall provide the capability to queue communications between services and applications.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1605	The system shall provide the capability to run process transactions.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1606	The system shall provide the capability to manage process transactions declaratively via system configurations.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1607	The system shall provide the capability to manage process transactions declaratively using a GUI.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1608	The system shall provide the capability to store process transactions configuration information in XML.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1609	The system shall provide the capability to execute pre-defined process transactions.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1610	The system shall provide the capability to manually commit and roll back process transactions.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1611	The system shall provide the capability to create communications between services or applications, internal or external, in XML form with published schemas.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1612	The system shall provide the capability to validate messages against the appropriate published schema.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1613	The system shall provide the capability to transform messages to different schemas.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1614	The system shall provide the capability to perform XML document-based routing between services or applications.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1615	The system shall provide the capability to support incremental implementations.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1616	The ESB shall support the capability to deploy services without disrupting system operations.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1617	The ESB shall support the capability to remove services without disrupting system operations that do not rely on the service which is being removed.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1618	The ESB shall support the capability to deploy applications without disrupting system operations.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1619	The ESB shall support the capability to remove applications without disrupting system operations that do not rely on the application which is being removed.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1620	The system shall provide the capability to support exception handling.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1621	The system shall provide the capability to generate compensating transactions for exceptions where possible.	Infrastructure	Enterprise Service Bus	R3 Should
RD-1622	The system shall store information related to the ESB in logs.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1623	The system shall store information about data types exchanged over the ESB in XML schema.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1624	The ESB shall support WSDL.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1625	The ESB shall support WS-Security.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1626	The ESB shall support WS-Reliability or WS-Reliable Messaging	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1627	The system shall store information about transactional operations in logs.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1629	The system shall store information about communications in logs.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1631	The system shall store information about business processes in logs.	Infrastructure	Enterprise Service Bus	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1632	The system shall support the capability to record information about business process execution in logs.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1634	The system shall provide the capability to perform integration configurations.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1635	The system shall provide the capability to manage integration configurations using a GUI.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1636	The system shall provide the capability to perform integration configurations in XML.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1637	The system shall provide the capability to store integration configuration information in XML.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1638	The system shall provide the capability to add redundancy to critical ESB functions.	Infrastructure	Enterprise Service Bus	R2 Must
RD-1640	The system shall provide the capability to impose rule-based security control over administrative tasks.	Infrastructure	Enterprise Service Bus	R3 Must
RD-1641	The system shall provide the capability to manage services or applications dynamically.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1643	The system shall provide the capability to enable services dynamically.	Infrastructure	Enterprise Service Bus	R2 Must
RD-1644	The system shall provide the capability to disable services dynamically.	Infrastructure	Enterprise Service Bus	R2 Must
RD-1645	The system shall provide the capability to manage business processes.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1646	The system shall provide the capability to support business process orchestration.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1648	The system shall provide the capability to terminate business processes that are being orchestrated.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1649	The system shall provide the capability to suspend business processes that are being orchestrated.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1650	The system shall provide the capability to resume business processes that are suspended.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1651	The system shall provide the capability to monitor ESB processes that are being orchestrated.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1652	The system shall provide the capability to monitor the business processes at all available statuses: active, suspended, terminated, and completed.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1653	The system shall provide the capability to monitor communication latencies.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1654	The system shall provide the capability to send notifications in the event of problems with ESB functions.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1656	The system shall provide the capability to perform configuration tasks via a Graphical User Interface (GUI) tool.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1657	The system shall provide the capability to perform administrative tasks via a GUI tool.	Infrastructure	Enterprise Service Bus	R1C2 Must
RD-1430	The system shall keep an audit log of all transactions in the system.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1431	The system shall create audit logs which contain sufficient information to establish what events occurred, the source(s) of the events, and the outcomes of the events.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1432	Audit logs shall contain logged events which each contain the date the event occurred.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1433	Audit logs shall contain logged events which each contain the time the event occurred.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1434	Audit logs shall contain logged events which contain the name of the component, application, or service that logged the event.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1435	Audit logs shall contain logged events which each contain a classification of the event by the event source.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1436	Audit logs shall contain logged events which each contain a classification of the event severity: Error, Information, or Warning in the system and application logs; Success Audit or Failure Audit in the security log.	Infrastructure	Event And Audit Logging	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1437	Audit logs shall contain logged events which each contain a number identifying the particular event type.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1438	Audit logs shall contain a description of the event.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1439	Audit logs shall contain a description of the event containing the user name of the user on whose behalf the event occurred.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1440	Audit logs shall contain a description of the event containing the name (IP address and DNS name) of the system on which the event occurred.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1441	Audit logs shall contain a description of the event involving significant problems such as a loss of data or functions.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1442	Audit logs shall contain a description of the event containing information about infrequent significant events that describe successful operations of major server services.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1443	Audit logs shall contain a description of the event containing warnings, events that are not necessarily significant, but that indicate possible future problems.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1444	Audit logs shall contain a description of the event containing an audit of the security access attempts to objects that were successful.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1445	Audit logs shall contain a description of the event containing an audit of the security access attempts to objects that failed.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1446	Audit logs shall contain additional data fields where binary data can be displayed in bytes or words.	Infrastructure	Event And Audit Logging	R2 Must
RD-1447	The system shall maintain a system log containing events logged by the system components.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1448	The system shall allow system logs to be viewed by all authorized users.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1449	The system shall have the capability to maintain a security log containing valid and invalid logon attempts as well as events related to resource use, such as creating, opening, or deleting files or other objects.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1450	The system shall allow security logs to be viewed by authorized users.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1452	The system shall maintain a security log containing events related to resource use, such as creating, opening, or deleting files or other objects.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1453	The system shall maintain an application log containing events logged by applications.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1454	The system shall allow applications logs to be viewed by authorized users.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1455	The system shall have an Audit Log manager for system administrator functions.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1456	The Audit Log manager application shall be searchable.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1457	The system shall provide the capability to log completed transaction information.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1458	The system shall provide the capability to view completed transaction.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1459	The system shall keep an audit log of user ordering (request) transactions.	Infrastructure	Event And Audit Logging	R1C3 Must
RD-1460	The system shall keep an audit log of system administration transactions.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1461	The system shall keep an audit log of security administrator transactions.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1462	The system shall keep an audit log of system access rights changes.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1463	The system shall keep an audit log of preservation processes.	Infrastructure	Event And Audit Logging	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1464	The system shall keep an audit log of deposited content activities.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1465	The system shall keep an audit log of harvested content activities.	Infrastructure	Event And Audit Logging	R1C4 Must
RD-1466	The system shall keep an audit log of converted content activities.	Infrastructure	Event And Audit Logging	R1C4 Must
RD-1467	The system shall keep an audit log of Content Originator ordering activities.	Infrastructure	Event And Audit Logging	R1C3 Must
RD-1468	The system shall keep an audit log of content authentication activities.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1469	The system shall keep an audit log of version control activities.	Infrastructure	Event And Audit Logging	R1C4 Must
RD-1470	The system shall keep an audit log of cataloging activities.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1471	The system shall keep an audit log of support activities (e.g., support status).	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1472	The system shall keep an audit log for data mining.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1473	The system shall have the capability to maintain integrity of audit logs.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1474	The system shall protect the audit log from unauthorized user modification.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1475	The system shall detect user attempts to edit audit logs.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1476	The system shall keep an audit log of attempts to access the system.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1477	The system shall keep an audit log of any detected breaches of security policy.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1480	The system shall store audit logs (e.g. audit trails) per GPO P825.33.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1481	The system shall manage audit log stores.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1482	The system shall save audit logs as specified in GPO Publication 825.33.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-3589	The system shall consolidate all audit logs using GPO's log consolidation tool.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-506	The system shall have the capability to create a log of all transactions and activities.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-865	The system shall not allow system log files to be changed.	Infrastructure	Event And Audit Logging	R1C2 Must
RD-1270	WIPs shall be protected from unauthorized alteration by user actions.	Infrastructure	Group Enforcement	R1C3 Must
RD-1281	SIPs shall be protected from unauthorized alteration by user actions.	Infrastructure	Group Enforcement	R1C2 Must
RD-1282	AIPs shall be protected from unauthorized alteration by user actions.	Infrastructure	Group Enforcement	R1C2 Must
RD-1292	ACPs shall be protected from unauthorized alteration by user actions.	Infrastructure	Group Enforcement	R1C2 Must
RD-1303	BPI shall be protected from unauthorized alteration by user actions.	Infrastructure	Group Enforcement	R1C3 Must
RD-1314	The system shall control access to data in storage based in the user's group.	Infrastructure	Group Enforcement	R1C2 Must
RD-2362	The system shall provide the capability for authorized users to access final approved versions of ACPs that are not in scope for GPO's dissemination programs.	Infrastructure	Group Enforcement	R1C2 Must
RD-3261	The system shall have the capability to restrict Service Providers' access to DIPs and pre-ingest bundles for jobs that they have not been awarded.	Infrastructure	Group Enforcement	R1C3 Must
RD-3262	The system shall have the capability to restrict Service Providers' access to DIPs for jobs that they have not been awarded.	Infrastructure	Group Enforcement	R1C3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3263	The system shall have the capability to restrict Service Providers' access to pre-ingest bundles for jobs that they have not been awarded.	Infrastructure	Group Enforcement	R1C3 Must
RD-1195	Each data center in the system shall be housed in a facility protected by physical security measures.	Infrastructure	Manage Security	R1C2 Must
RD-1315	The system shall prefer the use of Lightweight Directory Access Protocol over Active Directory wherever possible.	Infrastructure	Manage Security	R1C2 Must
RD-1386	The system shall support a configurable minimum password length parameter, settable by authorized system administrators. The minimum value allowable for this parameter is eight (8).	Infrastructure	Manage Security	R1C2 Must
RD-1387	The system shall permit stronger authentication techniques to be used for system and security administrators (such as longer and/or more complex passwords, public key certificate, and token based authentication).	Infrastructure	Manage Security	R1C2 Must
RD-1388	The system shall permit authorized users to create a unique user identity for access to the system.	Infrastructure	Manage Security	R1C2 Must
RD-1389	The system shall enforce uniqueness of user identity so that no two users can use the exact same identity.	Infrastructure	Manage Security	R1C2 Must
RD-1390	The system shall be capable of Identity Management system functionality to facilitate provisioning of user identities.	Infrastructure	Manage Security	R1C2 Must
RD-1399	The system shall comply with GPO authentication policies specified in P825.33.	Infrastructure	Manage Security	R1C2 Must
RD-1401	The system shall have the capability to support up to 2048-bit RSA public/private key generation (asymmetric algorithm).	Infrastructure	Manage Security	R1C4 Must
RD-1485	The system shall support the capability of maintaining user privacy in accordance with GPO Publication 825.33.	Infrastructure	Manage Security	R1C2 Must
RD-1486	The system shall support the capability of maintaining user privacy in accordance with Title 5 USC Sec. 552a (Records maintained on individuals).	Infrastructure	Manage Security	R1C2 Must
RD-1487	The system shall support the capability of maintaining access privacy (e.g., Search, Request).	Infrastructure	Manage Security	R1C2 Must
RD-1488	The system shall support the capability of maintaining support privacy (e.g., user identity).	Infrastructure	Manage Security	R1C2 Must
RD-1489	The system shall support the capability of maintaining Content Originator ordering privacy.	Infrastructure	Manage Security	R1C3 Must
RD-1490	The system shall provide measures that preclude a single authorized administrator from listing an end user's orders.	Infrastructure	Manage Security	R2 Must
RD-1492	The system shall support the capability of maintaining confidentiality of user data (e.g., passwords).	Infrastructure	Manage Security	R1C2 Must
RD-1493	The system shall have the capability to provide confidentiality of user authentication data exchanged through external interfaces.	Infrastructure	Manage Security	R1C2 Must
RD-1496	The system shall use a minimum 128 bit key length for all symmetric encryption operations.	Infrastructure	Manage Security	R1C4 Must
RD-1497	The system shall have the capability to provide confidentiality of user data, including confidentiality of user authentication data stored within the system (e.g., passwords).	Infrastructure	Manage Security	R1C2 Must
RD-1498	The system shall support the capability of maintaining confidentiality of sensitive content in accordance with NIST and FIPS requirements for Sensitive But Unclassified (SBU) content.	Infrastructure	Manage Security	R1C2 Must
RD-1499	The system shall provide a method of protecting confidential and private FDsys system data. (e.g., passwords, private user data, PII)	Infrastructure	Manage Security	R1C2 Must
RD-1551	The system shall have the capability to support the following industry integrity and authentication standards.	Infrastructure	Manage Security	R3 Must
RD-1552	The system shall have the capability to support the RSA Digital Signature in accordance with IETF RFC 3447.	Infrastructure	Manage Security	R1C4 Must
RD-1553	The system shall have the capability to support Public Key Infrastructure (PKI) PKCS #1 standards.	Infrastructure	Manage Security	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1554	The system shall have the capability to support Public Key Infrastructure (PKI) PKCS #7 standards.	Infrastructure	Manage Security	R1C4 Must
RD-1555	The system shall have the capability to support Public Key Infrastructure (PKI) PKCS #11 standards.	Infrastructure	Manage Security	R1C4 Must
RD-1556	The system shall have the capability to support Public Key Infrastructure (PKI) PKCS #12 standards.	Infrastructure	Manage Security	R1C4 Must
RD-1557	The system shall have the capability to support the International Telephone Union (ITU) X.509 v3 standard for certificate format.	Infrastructure	Manage Security	R1C4 Must
RD-1558	The system shall have the capability to support the IETF Public Key Infrastructure Exchange (PKIX) X.509 v3 standards for certificate compatibility.	Infrastructure	Manage Security	R1C4 Must
RD-1559	The system shall have the capability to support the Keyed-Hash Message Authentication Code (HMAC) standard as specified in FIPS Pub 198.	Infrastructure	Manage Security	R1C2 Must
RD-1560	The system shall have the capability to support the Cyclical Redundancy Checking (CRC) 32 (CRC-32) standard, to include Cyclic Redundancy Checking (CRC) and checksum.	Infrastructure	Manage Security	R1C2 Must
RD-1561	The system shall have the capability to support the FIPS 180-2 Secure Hash Algorithm (SHA) SHA-1 standard.	Infrastructure	Manage Security	R1C2 Must
RD-1562	The system shall the capability to support the FIPS 180-2 Secure Hash Algorithm (SHA) SHA-256 standard.	Infrastructure	Manage Security	R1C2 Must
RD-1563	The system shall have the capability to support the FIPS 180-2 Secure Hash Algorithm (SHA) SHA-384 standard.	Infrastructure	Manage Security	R1C2 Must
RD-1564	The system shall have the capability to support the FIPS 180-2 Secure Hash Algorithm (SHA) SHA-512 standard.	Infrastructure	Manage Security	R3 Must
RD-1565	The system shall have the capability to support the XML Digital Signature standards defined in RFC 3275 and XMLDSIG.	Infrastructure	Manage Security	R1C2 Must
RD-1566	The system shall have the capability to support the following confidentiality standards.	Infrastructure	Manage Security	R1C2 Must
RD-1567	The system shall have the capability to support the FIPS 197 Advanced Encryption Standard (AES).	Infrastructure	Manage Security	R1C2 Must
RD-1568	The system shall have the capability to support the ANSI X9.52 Triple Data Encryption Standard (TDES).	Infrastructure	Manage Security	R1C2 Must
RD-1569	The system shall have the capability to support the Secure Sockets Layer (SSL) version 3 / Transport Layer Security (TLS) standards per the guidelines in NIST SP 800-52.	Infrastructure	Manage Security	R1C2 Must
RD-1570	The system shall have the capability to comply with FIPS 140-2.	Infrastructure	Manage Security	R1C2 Must
RD-1572	The system shall have the capability to support the following access control standards.	Infrastructure	Manage Security	R1C2 Must
RD-1573	The system shall have the capability to support the Lightweight Directory Access Protocol (LDAP) Internet Engineering Task Force (IETF) Request for Comments (RFC) 2251.	Infrastructure	Manage Security	R1C2 Must
RD-1574	The system shall have the capability to support the International Telephone Union (ITU) X.500 standards.	Infrastructure	Manage Security	R1C2 Must
RD-1575	The system shall have the capability to support the Security and Access Markup Language (SAML) version 2 standard as specified by OASIS.	Infrastructure	Manage Security	R1C2 Must
RD-3090	Information collected and maintained shall comply with "Records maintained on individuals", Title 5 U.S. Code Sec. 552a, 2000 edition.	Infrastructure	Manage Security	R1C2 Must
RD-3091	Information collected and maintained shall comply with H.R. 2458, E-Government Act of 2002.	Infrastructure	Manage Security	R1C2 Must
RD-3593	The system shall have the capability to support authentication standards as specified in the Government Printing Office Authentication White Paper.	Infrastructure	Manage Security	R1C2 Must
RD-3594	The system shall have the capability to support authentication standards as specified in NIST 500-156.	Infrastructure	Manage Security	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3600	The system shall have the capability to support the NIST 800-64 standard.	Infrastructure	Manage Security	R1C2 Must
RD-3601	The system shall have the capability to support the NIST 800-26.	Infrastructure	Manage Security	R1C2 Must
RD-770	The system shall provide the capability to use passwords to verify the identity of authorized users.	Infrastructure	Manage Security	R1C2 Must
RD-771	The system shall provide the capability to use PKI certificates to verify the identity of authorized users.	Infrastructure	Manage Security	R1C4 Must
RD-772	The system shall provide the capability to verify the authorization level of authorized users to perform requested functions.	Infrastructure	Manage Security	R1C2 Must
RD-773	The system shall provide the capability to validate credentials (e.g., digital certificate) of authorized users.	Infrastructure	Manage Security	R1C4 Must
RD-1542	The system shall have the following security capabilities to permit the system to be operated at a hosting vendor site, at GPO's sole discretion.	Infrastructure	Network Security	R1C2 Must
RD-1543	Mutually authenticated, high speed connection between GPO offices and hosting site shall be utilized.	Infrastructure	Network Security	R1C2 Must
RD-1544	Encrypted connection using industry standard IPSEC Virtual Private Network (VPN) and strong (128 bit key minimum) encryption shall be utilized.	Infrastructure	Network Security	R1C2 Must
RD-1405	The system shall permit authorized security administrators to create roles.	Infrastructure	Security Administration	R1C2 Must
RD-1406	The system shall permit authorized security administrators and delegated authorities to assign users to customized roles.	Infrastructure	Security Administration	R1C2 Must
RD-1407	The system shall provide access control limitations to support data mining .	Infrastructure	Security Administration	R1C2 Must
RD-1409	The system shall allow authorized security administrators and delegated authorities to assign users to roles for access to system functions.	Infrastructure	Security Administration	R1C2 Must
RD-1410	The system shall allow authorized security administrators to assign users to groups for access to content.	Infrastructure	Security Administration	R1C2 Must
RD-1413	The system shall provide the capability to create user accounts.	Infrastructure	Security Administration	R1C2 Must
RD-1414	The system shall provide the capability to create group accounts.	Infrastructure	Security Administration	R1C2 Must
RD-1415	The system shall provide the capability to access user accounts.	Infrastructure	Security Administration	R1C2 Must
RD-1416	The system shall provide the capability to delete user accounts.	Infrastructure	Security Administration	R1C2 Must
RD-1417	The system shall provide the capability to suspend user accounts.	Infrastructure	Security Administration	R1C2 Must
RD-1418	The system shall provide the capability to reactivate suspended user accounts.	Infrastructure	Security Administration	R1C2 Must
RD-1419	The system shall provide the capability for the renewal of user registrations.	Infrastructure	Security Administration	R1C2 Must
RD-1420	The system shall have the capability to expire user accounts, configurable by security administrators.	Infrastructure	Security Administration	R1C2 Must
RD-1427	The system shall provide the capability for authorized users to manage (add, modify, delete) user account information.	Infrastructure	Security Administration	R1C2 Must
RD-1428	The system shall have the capability to provide secure interfaces for FDsys operations.	Infrastructure	Security Administration	R1C2 Must
RD-1504	The system shall provide an administrative graphical user interface to perform user administration.	Infrastructure	Security Administration	R1C2 Must
RD-1505	The system shall provide an administrative graphical user interface to perform security administration.	Infrastructure	Security Administration	R1C2 Must
RD-1507	The system shall have the capability for authorized security administrators to implement system security policy.	Infrastructure	Security Administration	R1C2 Must
RD-1511	System security policy parameters shall include minimum passwords lengths.	Infrastructure	Security Administration	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1512	System security policy parameters shall include authorized encryption algorithms.	Infrastructure	Security Administration	R1C2 Must
RD-1513	The system shall be flexible enough to incorporate additional, GPO-defined system security policy parameters.	Infrastructure	Security Administration	R1C2 Must
RD-1514	The system shall have the capability for authorized security administrators to maintain system security policy.	Infrastructure	Security Administration	R1C2 Must
RD-1518	The system shall provide the capability to define tasks that require more than one authorized administrator to perform (e.g., setting or changing critical system security policies, two person integrity (TPI)).	Infrastructure	Security Administration	R1C4 Must
RD-1519	The system shall have the capability to enforce the separation of functions through assigned roles.	Infrastructure	Security Administration	R1C2 Must
RD-1520	The system shall provide the capability to partition security administration into groups.	Infrastructure	Security Administration	R1C2 Must
RD-1521	The system shall provide the capability to limit security administrator's authority to assigned groups.	Infrastructure	Security Administration	R1C2 Must
RD-2387	The system shall provide the capability for authorized users to set required fields in user accounts.	Infrastructure	Security Administration	R1C2 Must
RD-2395	The system shall associate registered users with at least one user group.	Infrastructure	Security Administration	R1C2 Must
RD-2399	The system shall provide the capability to manage user records.	Infrastructure	Security Administration	R1C2 Must
RD-2401	The system shall provide the capability for authorized users to manage the following user preferences:	Infrastructure	Security Administration	R1C3 Should / R2 Must
RD-2410	The system shall provide the capability for authorized users to manage other users' preferences.	Infrastructure	Security Administration	R1C3 Should / R2 Must
RD-2411	The system shall provide the capability for GPO to establish and manage default user preferences.	Infrastructure	Security Administration	R1C2 Should / R2 Must
RD-3595	The system shall provide the capability for authorized users to manage required fields in user accounts.	Infrastructure	Security Administration	R1C2 Must
RD-1516	The system shall provide the capability for authorized security administrators to monitor system security policy settings.	Infrastructure	Security Monitoring	R1C2 Must
RD-1517	The system shall provide the capability for authorized security administrators to monitor system security policy enforcement.	Infrastructure	Security Monitoring	R1C2 Must
RD-1193	The system shall be capable of providing a secure repository environment for all storage.	Infrastructure	Storage Management	R1C2 Must
RD-1194	Near-line storage media shall provide the capability to preserve data integrity and quality for no less than 10 years in a data center environment.	Infrastructure	Storage Management	R1C2 Must
RD-1200	The system shall support the capability to include multiple storage classes.	Infrastructure	Storage Management	R2 Must
RD-1201	The system shall support the capability to add additional storage classes in the future without a major redesign.	Infrastructure	Storage Management	R2 Must
RD-1202	The system shall support the capability to transparently migrate data from one storage class to another based on system policies.	Infrastructure	Storage Management	R2 Must
RD-1203	The system shall support the capability for authorized users to configure the policies used by the system to migrate data from one class of storage to another.	Infrastructure	Storage Management	R1C2 Must
RD-1204	The system shall support the capability for authorized users to set storage policies for selected content packages.	Infrastructure	Storage Management	R2 Must
RD-1206	The system shall have the capability to store data dynamically in external Content Delivery Networks (CDN) based on hit rate/criticality of content.	Infrastructure	Storage Management	R2 Must
RD-1207	The system shall support the capability for authorized users to designate data for storage in a Content Delivery Network.	Infrastructure	Storage Management	R1C2 Must
RD-1210	The system shall have the capability to utilize external storage Service Providers.	Infrastructure	Storage Management	R1C2 Must
RD-1243	Failover Storage shall support an alternate path (e.g., ability to automatically switch between input/output (I/O) paths in the event of a failure in one of the paths).	Infrastructure	Storage Management	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1263	Long-term Permanent Archival Storage design shall have the off-line storage capability for scaling to multiple Petabytes of data.	Infrastructure	Storage Management	R1C2 Must
RD-1264	Long-term Permanent Archival Storage shall have indexing capability for multiple Petabytes of data.	Infrastructure	Storage Management	R1C2 Must
RD-1275	WIP Storage shall contain content, metadata, and BPI.	Infrastructure	Storage Management	R1C3 Must
RD-1276	Archival Information Package (AIP) Storage	Infrastructure	Storage Management	R1C2 Must
RD-1277	The system shall provide the capability to write all AIPs to archival media for off site storage.	Infrastructure	Storage Management	R1C2 Must
RD-1287	AIP Storage shall exist in isolation of other system stores.	Infrastructure	Storage Management	R1C2 Must
RD-1289	AIP Storage shall contain both content and metadata.	Infrastructure	Storage Management	R1C2 Must
RD-1300	ACPs shall contain both content and metadata.	Infrastructure	Storage Management	R1C2 Must
RD-1316	The system shall be able to ingest files stored on disk systems connected directly to the system.	Infrastructure	Storage Management	R2 Must
RD-1317	The system shall provide the capability to read files stored in common operating system formats.	Infrastructure	Storage Management	R2 Must
RD-1318	The system shall be able to ingest files stored in a FAT file system.	Infrastructure	Storage Management	R2 Must
RD-1319	The system shall be able to ingest files stored in a FAT32 file system.	Infrastructure	Storage Management	R2 Must
RD-1320	The system shall be able to ingest files stored in a VFAT file system.	Infrastructure	Storage Management	R2 Must
RD-1321	The system shall be able to ingest files stored in a NTFS file system.	Infrastructure	Storage Management	R2 Must
RD-1322	The system shall be able to ingest files stored in a HPFS file system.	Infrastructure	Storage Management	R2 Must
RD-1323	The system shall be able to ingest files stored in a EXT2 file system.	Infrastructure	Storage Management	R2 Must
RD-1324	The system shall be able to ingest files stored in a EXT3 file system.	Infrastructure	Storage Management	R2 Must
RD-1325	The system shall be able to ingest files stored in a EXT4 file system.	Infrastructure	Storage Management	R2 Must
RD-1326	The system shall be able to ingest files stored in a HFS Plus file system.	Infrastructure	Storage Management	R2 Must
RD-1327	The system shall be able to ingest files stored in a JFS2 file system.	Infrastructure	Storage Management	R2 Must
RD-1328	The system shall be able to ingest files stored in a UFS file system.	Infrastructure	Storage Management	R2 Must
RD-1329	The system shall utilize common Redundant Array of Independent Disks (RAID) Disk Data Format (DDF) architecture.	Infrastructure	Storage Management	R1C2 Must
RD-1337	The system storage shall support ANSI INCITS 388-2004 Storage Management Initiative Specification.	Infrastructure	Storage Management	R2 Must
RD-1338	The system back-up tapes shall conform to Linear Tape-Open (LTO) standard.	Infrastructure	Storage Management	R1C4 Must
RD-1359	The system shall allow users to reconfigure RAID levels without vendor assistance.	Infrastructure	Storage Management	R2 Must
RD-1361	The system shall automatically allocate stand-by drives to replace drives that have failed.	Infrastructure	Storage Management	R1C2 Must
RD-1363	The system shall provide the capability to hot swap power supplies when a power supply has failed.	Infrastructure	Storage Management	R1C2 Must
RD-1364	The system shall provide the capability to hot swap cooling fans when a cooling fan has failed.	Infrastructure	Storage Management	R1C2 Must
RD-1365	The system shall provide the capability to hot swap disk drives in disk storage systems when a disk drive has failed.	Infrastructure	Storage Management	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1366	The system shall provide the capability to hot swap blade servers when a blade server has failed.	Infrastructure	Storage Management	R1C4 Must
RD-1367	The system shall have the ability to dynamically move data to improve system performance.	Infrastructure	Storage Management	R1C2 Must
RD-1368	The storage systems shall provide the capability to upgrade controller microcode without shutting down the storage system.	Infrastructure	Storage Management	R2 Must
RD-1370	The system shall allow for securing of allocatable storage.	Infrastructure	Storage Management	R1C2 Must
RD-1371	The system shall allow encryption of content.	Infrastructure	Storage Management	R3 Must
RD-1374	The system shall support the management of heterogeneous storage architectures (e.g. direct attached storage (DAS), network attached storage (NAS), storage area network (SAN)).	Infrastructure	Storage Management	R1C2 Must
RD-1375	The system shall provide the capability to automatically allocate additional storage when a user configurable threshold is crossed.	Infrastructure	Storage Management	R1C2 Must
RD-1376	The system shall be able to manage any infrastructure storage device attached to the system.	Infrastructure	Storage Management	R1C2 Must
RD-1377	The system shall allow manual compression of data at various compression levels.	Infrastructure	Storage Management	R1C2 Must
RD-1378	The system shall provide the capability to allocate storage on new devices after they have been identified by the system and formatted for use.	Infrastructure	Storage Management	R1C2 Must
RD-1781	The system shall have the capability to manage storage (e.g., delete files and reports at a defined time).	Infrastructure	Storage Management	R2 Must
RD-260	The system shall support the creation of AIPs which are independent of any particular hardware and software component.	Infrastructure	Storage Management	R1C2 Must
RD-262	The system shall provide the capability to store content in an AIP independent of the content's digital format.	Infrastructure	Storage Management	R1C2 Must
RD-3592	The system shall allow automated compression of data at various compression levels.	Infrastructure	Storage Management	R1C2 Must
RD-509	The system shall have the ability to store AIPs in a preservation repository environment.	Infrastructure	Storage Management	R1C2 Must
RD-637	The system shall provide a digital archival repository environment which is based on open-standards architecture.	Infrastructure	Storage Management	R1C2 Must
RD-638	The repository environment shall keep AIPs separate from working or production copies.	Infrastructure	Storage Management	R1C2 Must
RD-1086	The system shall replicate workflow data to failover location(s).	Infrastructure	Storage Replication	R1C2 Must
RD-1233	Failover Storage shall provide the fault tolerance required to allow the system to survive a localized disaster.	Infrastructure	Storage Replication	R1C2 Must
RD-1234	Failover Storage shall be able to reconstitute and switch-over to alternate systems at a remote site in the event of local catastrophic damage.	Infrastructure	Storage Replication	R1C2 Must
RD-1235	The system shall replicate all system data to a disaster recovery site.	Infrastructure	Storage Replication	R1C2 Must
RD-1237	Failover Storage shall allow the switchover to redundant components via user action.	Infrastructure	Storage Replication	R1C2 Must
RD-1238	Failover Storage shall allow the switchover to redundant components automatically in case of failure.	Infrastructure	Storage Replication	R1C2 Must
RD-1239	The system shall replicate all content packages to a disaster recovery site.	Infrastructure	Storage Replication	R1C2 Must
RD-1240	The system shall replicate all BPI to a disaster recovery site.	Infrastructure	Storage Replication	R1C3 Must
RD-640	The system shall maintain one on more backups of the repository environment consistent with the overall FDsys storage requirements.	Infrastructure	Storage Replication	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-866	The system shall have the capability to certify integrity of content during backup and other system processes.	Infrastructure	Storage Replication	R1C2 Must
RD-39	The system shall support an average peak time availability of 99.7%.	Infrastructure	System Availability	R1C2 Must
RD-1085	The system shall prevent the loss of workflow data.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1087	The system shall allow the frequency of backup processes to be controlled by authorized users.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1088	The system shall allow the backup processes to be controlled automatically or manually by authorized users.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1089	The system shall backup all necessary data required to retrieve workflow data to its original state in the event of a system failure.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1090	The system shall perform workflow backup processes without interruption to users.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1245	Back-up Retrieval Media Storage shall be able to accomplish periodic backup on mass removable storage media.	Infrastructure	System Backup / Restore	R1C4 Must
RD-1246	Back-up Retrieval Media Storage shall allow users to manage periodic backup schedules.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1247	Back-up Retrieval Media Storage shall allow backups on multiple types of mass removable storage media.	Infrastructure	System Backup / Restore	R1C4 Must
RD-1248	Back-up Retrieval Media Storage shall be able to accomplish a full back-up of all critical data in less than six hours or scheduled periodically over 24 hours.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1249	Back-up Retrieval Media Storage shall allow users to manage which data is listed as critical.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1250	Back-up Retrieval Media Storage shall allow users to manage the backup schedule.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1251	Back-up Retrieval Media Storage shall not interfere with current system processes.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1253	Back-up Retrieval Media Storage shall support mirroring the write data in cache as a method of data protection.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1254	Back-up Retrieval Media Storage shall allow users to manage which data should be backed up.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1255	Back-up Retrieval Media Storage shall support proactively testing data for errors even when the cache or disk is inactive, so that problems can be detected before they can disrupt data flow.	Infrastructure	System Backup / Restore	R3 Must
RD-1256	Back-up Retrieval Media Storage shall allow users the ability to both schedule and manually test data for errors even when the cache or disk is inactive.	Infrastructure	System Backup / Restore	R3 Must
RD-1257	Back-up Retrieval Media Storage shall support the process of copying data to a second disk array.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1524	The system shall provide appropriate backup capability to ensure recovery to meet customer and GPO needs.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1534	The system shall back up system applications at a frequency as determined by business requirements.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1535	The system shall back up system data at a frequency as determined by business requirements.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1537	The system applications shall be backed up at off-site storage location.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1538	The system data shall be backed up at off-site storage location.	Infrastructure	System Backup / Restore	R1C2 Must
RD-1540	The system shall maintain data integrity during backup processing.	Infrastructure	System Backup / Restore	R1C2 Must
RD-11	The system shall support the capability to change key parameters affecting the operation of the system without redesigning the system.	Infrastructure	System Flexibility	R1C2 Must
RD-12	The system shall support the capability to accommodate changes in hardware technologies without requiring major reengineering or design changes.	Infrastructure	System Flexibility	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1288	The system shall support the capability to migrate AIP content to future storage technologies.	Infrastructure	System Flexibility	R1C2 Must
RD-13	The system shall support the capability to accommodate changes in software technologies without requiring major reengineering or design changes.	Infrastructure	System Flexibility	R1C2 Must
RD-1330	The system shall conform to commonly used, industry standard protocols.	Infrastructure	System Flexibility	R2 Must
RD-1331	The system shall support the capability to interface with industry standard protocols.	Infrastructure	System Flexibility	R2 Must
RD-1332	The system shall use industry standard protocols when there is one that meets the system requirements.	Infrastructure	System Flexibility	R2 Must
RD-1333	The system shall use non-standard protocols only when there is no industry standard that meets the system requirements.	Infrastructure	System Flexibility	R2 Must
RD-1539	The system shall interface with designated GPO Service Providers (e.g. Oracle Financials).	Infrastructure	System Flexibility	R1C2 Must
RD-1541	The system shall have no restrictions that would prevent the system from being operated at a hosting vendor site, at GPO's sole discretion, at any point in the future.	Infrastructure	System Flexibility	R1C2 Must
RD-1547	The system shall check content for malicious code (e.g., worms and viruses) prior to ingest to maintain integrity.	Infrastructure	System Flexibility	R1C2 Must
RD-1548	The system shall utilize GPO virus scanner technology.	Infrastructure	System Flexibility	R1C2 Must
RD-1549	If malicious code is detected in content, it shall be placed into a quarantine area for GPO inspection.	Infrastructure	System Flexibility	R1C2 Must
RD-16	The system shall support the capability to accommodate changes in personnel without requiring major reengineering or design changes.	Infrastructure	System Flexibility	R1C2 Must
RD-17	The system shall support the capability to accommodate changes in system locations without requiring major reengineering or design changes.	Infrastructure	System Flexibility	R1C2 Must
RD-19	The system shall have the ability to handle additional kinds of content over time, not limited to specific types that exist today.	Infrastructure	System Flexibility	R1C2 Must
RD-2	The system shall provide for the use of internal and external open interfaces.	Infrastructure	System Flexibility	R1C2 Must
RD-20	The system shall provide the ability to ingest content regardless of its digital format.	Infrastructure	System Flexibility	R1C2 Must
RD-21	The system shall provide the ability to store content regardless of its digital format.	Infrastructure	System Flexibility	R1C2 Must
RD-2266	The system shall provide open and interoperable access to content.	Infrastructure	System Flexibility	R1C2 Must
RD-2267	The system shall provide open and interoperable access to metadata.	Infrastructure	System Flexibility	R1C2 Must
RD-23	The system shall provide support for content management lifecycle processes for harvested, converted and deposited content.	Infrastructure	System Flexibility	R2 Must
RD-2383	The system shall provide the capability to store and manage a number of user records that is only limited by available storage.	Infrastructure	System Flexibility	R1C2 Must
RD-2384	The system shall have the capability to store an unlimited number of user records without software re-design.	Infrastructure	System Flexibility	R1C2 Must
RD-2385	The system shall have the capability to manage an unlimited number of user records without software redesign.	Infrastructure	System Flexibility	R1C2 Must
RD-24	The system shall enable GPO to tailor content-based services to suit its customers needs and enable GPO to implement progressive improvements in its business process over time.	Infrastructure	System Flexibility	R2 Must
RD-25	The system shall enable GPO to tailor content-based services to suit its customers needs.	Infrastructure	System Flexibility	R3 Must
RD-26	The system shall enable GPO to tailor content-based services to implement progressive improvements in business process.	Infrastructure	System Flexibility	R3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3	The system may provide for the use of proprietary interfaces only when open interfaces are not available or do not meet system requirements.	Infrastructure	System Flexibility	R1C2 Must
RD-3597	The system shall have the capability to send notifications.	Infrastructure	System Flexibility	R1C2 Must
RD-3598	The system shall have the capability to send alerts.	Infrastructure	System Flexibility	R1C2 Must
RD-36	The system shall be available for use at all GPO locations.	Infrastructure	System Flexibility	R1C2 Must
RD-3603	The system shall provide open and interoperable access to BPI.	Infrastructure	System Flexibility	R1C3 Must
RD-4	The system shall provide an architecture that allows preservation of content independent of any specific hardware and software that was used to produce them.	Infrastructure	System Flexibility	R1C2 Must
RD-5	The system shall use plug-in components that can be replaced with minimal impact to remaining components as workload and technology change.	Infrastructure	System Flexibility	R2 Must
RD-511	AIPs shall remain free from corruption as GPO undergoes changes in information technology and infrastructure.	Infrastructure	System Flexibility	R1C2 Must
RD-512	AIPs shall remain accessible as GPO undergoes changes in information technology and infrastructure.	Infrastructure	System Flexibility	R1C2 Must
RD-52	The Application Programmer Interfaces of the system shall be based on open standards.	Infrastructure	System Flexibility	R1C2 Must
RD-6	The system shall accommodate changes in technologies and policies without requiring major re-engineering or design changes.	Infrastructure	System Flexibility	R1C2 Must
RD-1196	Each data center in the system shall be protected from power failures for the time required to safely power down each system component.	Infrastructure	System Monitoring	R1C2 Must
RD-1197	Each data center in the system shall be equipped with power failure sensors capable of notifying users when facility power has failed.	Infrastructure	System Monitoring	R1C2 Must
RD-1199	Each data center in the system shall be equipped with environment sensors capable of notifying users when out of tolerance conditions are imminent.	Infrastructure	System Monitoring	R1C2 Must
RD-1335	The system shall allow interaction with management information bases (MIB) via SNMP.	Infrastructure	System Monitoring	R1C2 Must
RD-1340	The system shall provide the capability to monitor the health of system components in real time.	Infrastructure	System Monitoring	R1C2 Must
RD-1341	The system shall monitor the health of the network components in real-time.	Infrastructure	System Monitoring	R1C2 Must
RD-1342	The system shall monitor the health of the system applications in real-time.	Infrastructure	System Monitoring	R1C2 Must
RD-1343	The system shall monitor the health of the storage components in real-time.	Infrastructure	System Monitoring	R1C2 Must
RD-1344	The system monitor the health of the processing components in real-time.	Infrastructure	System Monitoring	R1C2 Must
RD-1345	The system shall monitor the health of the operating system in real-time.	Infrastructure	System Monitoring	R1C2 Must
RD-1346	The system shall provide the capability for the user to configure the upper and lower bounds for system parameters being monitored.	Infrastructure	System Monitoring	R1C2 Must
RD-1347	The system shall have the ability to send notifications and alerts to users via multiple channels should a performance problem, failure condition or impending failure be detected.	Infrastructure	System Monitoring	R1C2 Must
RD-1348	The system shall send alerts and notifications to authorized users when a performance problem is detected.	Infrastructure	System Monitoring	R1C2 Must
RD-1349	The system shall send alerts and notifications to users when a failure condition is detected.	Infrastructure	System Monitoring	R1C2 Must
RD-1350	The system shall send alerts and notifications to users when a failure is impending.	Infrastructure	System Monitoring	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1352	The system shall send alerts to the appropriate user screen.	Infrastructure	System Monitoring	R1C2 Must
RD-1353	The system shall send notifications to the appropriate e-mail.	Infrastructure	System Monitoring	R1C2 Must
RD-1354	The system shall send notifications via additional methods in the future.	Infrastructure	System Monitoring	R2 Must
RD-1355	The system shall allow the users to configure the problem severity level that triggers a user notification.	Infrastructure	System Monitoring	R1C2 Must
RD-1356	The system shall have the capability to monitor real-time performance of the system in terms of service levels.	Infrastructure	System Monitoring	R1C2 Must
RD-1357	The system shall provide storage usage metrics that allow projection of future storage needs.	Infrastructure	System Monitoring	R3 Must
RD-1358	The system shall have the capability to monitor a Service Level Agreement for an externally hosted data store.	Infrastructure	System Monitoring	R1C2 Must
RD-3599	The system shall have the capability to escalate notifications to alerts where possible.	Infrastructure	System Monitoring	R1C2 Must
RD-1198	Each data center in the system shall be equipped with HVAC capacity equal to 50% greater than the sum of the BTUs produced by all system equipment located in that data center.	Infrastructure	System Performance	R1C2 Must
RD-1269	The response time for WIPs shall be 2 seconds or less.	Infrastructure	System Performance	R1C3 Must
RD-1278	The processing time to convert SIPs to ACPs after submission to the system shall be 2 seconds or less.	Infrastructure	System Performance	R1C2 Must
RD-1279	The response time for AIPs stored in on line storage shall be 2 seconds or less.	Infrastructure	System Performance	R1C2 Must
RD-1291	The response time for ACPs shall be 2 seconds or less.	Infrastructure	System Performance	R1C2 Must
RD-1302	The response time for BPI shall be 2 seconds or less.	Infrastructure	System Performance	R1C3 Must
RD-18	The system shall provide the capability to scale to 50 Petabytes of storage without requiring redesign of the system.	Infrastructure	System Performance	R1C2 Must
RD-3327	The time required to deliver via http download a DIP created from an AIP in online storage that contains a 100 KB (TBS) screen optimized PDF to an average PC (TBS) connected to the GPO Intranet running Internet Explorer 6 shall be 18 seconds (TBS) or less.	Infrastructure	System Performance	R1C2 Must
RD-340	The access time for an ACP shall be as less than or equal to the access time for its corresponding AIP.	Infrastructure	System Performance	R1C2 Must
RD-3591	The response time for submitting a package to the system and getting a response shall be 2 seconds or less.	Infrastructure	System Performance	R1C2 Must
RD-3602	The system shall ensure that the time from the last processing activity made in order to finalize a package from a change request, to the first byte sent to be made publicly available will be less than 5 minutes.	Infrastructure	System Performance	R1C2 Must
RD-3605	The number of files in a batch submission shall not be limited by the system, but will only be limited by the capabilities of the underlying computing platform (hardware, storage, and operating systems).	Infrastructure	System Performance	R1C2 Must
RD-38	The system shall provide the capability to maintain required response times when there are 20,000 concurrent users performing a mix of operations that represents peak time operational use.	Infrastructure	System Performance	R1C2 Must
RD-42	The system shall provide a response to the user within 2 seconds of a user on the GPO intranet initiating an operation.	Infrastructure	System Performance	R1C2 Must
RD-679	The system shall provide the capability to support 1 trillion Digital Objects without software redesign.	Infrastructure	System Performance	R1C2 Must
RD-3326	The time required to deliver via http download a DIP created from an ACP that contains a 100 KB (TBS) screen optimized PDF to an average PC (TBS) connected to the GPO Intranet running Internet Explorer 6 shall be 15 seconds (TBS) or less.	Infrastructure	System Performance	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1394	A user shall only be allowed to manage attributes associated with their own user identity.	Infrastructure	User Registration	R1C3 Must
RD-1395	The system shall display a message to users if they fail to authenticate.	Infrastructure	User Registration	R1C2 Must
RD-1396	The system shall permit access to a default workbench for public End Users, which does not require them to login.	Infrastructure	User Registration	R2 Must
RD-1421	The system shall provide the capability for users to request that their accounts be cancelled.	Infrastructure	User Registration	R1C3 Must
RD-1422	The system shall provide the capability for users to update their account information.	Infrastructure	User Registration	R1C3 Must
RD-1424	The system shall provide a means to ensure that users cannot view information of other users unless authorized.	Infrastructure	User Registration	R1C2 Must
RD-1425	The system shall provide a means to ensure that users cannot modify information of other users unless authorized.	Infrastructure	User Registration	R1C2 Must
RD-1426	The system shall securely store personal information (e.g. user names and passwords).	Infrastructure	User Registration	R1C2 Must
RD-2366	The system shall provide access to public End Users that does not require them to log-in to the system.	Infrastructure	User Registration	R1C2 Must
RD-2367	The system shall provide access to public End Users that does not require them to register with the system.	Infrastructure	User Registration	R1C2 Must
RD-2380	The system shall provide the capability for users to register with the system.	Infrastructure	User Registration	R1C2 Must
RD-2381	The system shall provide the capability to establish a user account for each registered user.	Infrastructure	User Registration	R1C2 Must
RD-2382	The system shall provide the capability to create user accounts for registered users.	Infrastructure	User Registration	R1C2 Must
RD-2388	The system shall provide the capability to record information submitted by users during registration with system.	Infrastructure	User Registration	R1C2 Must
RD-2390	The system shall have the capability to collect name from the user during registration (e.g., honorific title, first name, last name, job title).	Infrastructure	User Registration	R1C2 Must
RD-2391	The system shall have the capability to collect contact information from the user during registration (e.g., address, city, state, zip code, country, phone number, fax number, email address).	Infrastructure	User Registration	R1C2 Must
RD-2396	The system shall provide the capability to collect role-based information from the user during registration.	Infrastructure	User Registration	R1C2 Must
RD-2975	The system shall provide GUIs that allow users to input and submit registration information and login to the system.	Infrastructure	User Registration	R1C3 Must
RD-3499	The system shall provide the capability to record information submitted by user during self-registration with the system.	Infrastructure	User Registration	R1C3 Must
RD-3500	The system shall provide the capability for users to self register with the system.	Infrastructure	User Registration	R1C3 Must
RD-10	The system shall prevent a user from performing a function unless the user possesses a user role permitting that function.	Infrastructure	User Roles	R1C2 Must
RD-1312	The system shall integrate with Unix and Windows based Directory Services (Lightweight Directory Access Protocol, Active Directory) to support role based access.	Infrastructure	User Roles	R1C2 Must
RD-1313	The system shall integrate with Lightweight Directory Access Protocol (LDAP).	Infrastructure	User Roles	R1C2 Must
RD-1391	The system shall be capable of Identity Management system functionality to provide users and system administrators with one single interface and control point for provisioning and managing user identities.	Infrastructure	User Roles	R1C2 Must
RD-1392	The system shall be capable of Identity Management system functionality to provide users and system administrators with one single interface and control point for provisioning and managing user identities that will be used to support the system's access control decisions.	Infrastructure	User Roles	R1C2 Must
RD-1403	The system shall have the capability to arbitrate access driven by GPO business policy.	Infrastructure	User Roles	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1411	The system shall allow the use of standards based LDAP technology for the role based access model.	Infrastructure	User Roles	R1C2 Must
RD-2081	The system shall ensure users are authorized to spend funds.	Infrastructure	User Roles	R1C3 Must
RD-2364	The system shall have the capability to provide access to system functions by user class.	Infrastructure	User Roles	R1C2 Must
RD-2394	Users may be members of multiple user groups simultaneously.	Infrastructure	User Roles	R1C2 Must
RD-266	The system shall provide the capability for authorized users to access AIPs for the purpose of disseminating DIPs from AIPs.	Infrastructure	User Roles	R1C2 Must
RD-2959	The system shall provide the capability for GPO to create workbenches for subsets of user classes.	Infrastructure	User Roles	R2 Must
RD-2962	The system shall allow all users to perform the actions allowed to unregistered users.	Infrastructure	User Roles	R1C2 Must
RD-2976	The system shall only display GUI functionality appropriate to the authorized user's role and group.	Infrastructure	User Roles	R1C2 Must
RD-2977	The system shall have the capability to assign access to system functionality based on a user role.	Infrastructure	User Roles	R1C2 Must
RD-2978	The system shall have the capability to assign access to system functionality based on user security settings.	Infrastructure	User Roles	R1C2 Must
RD-3033	The system shall provide a default interface for System Administrators that is based on their user role.	Infrastructure	User Roles	R1C2 Must
RD-3042	The system shall provide a default interface for Operations Managers that is based on their user role.	Infrastructure	User Roles	R1C2 Must
RD-3590	The system shall have the capability to integrate with the enterprise directory management service application.	Infrastructure	User Roles	R1C2 Must
RD-3596	The system shall allow users to be members of multiple user roles simultaneously.	Infrastructure	User Roles	R1C2 Must
RD-7	The system shall support multiple user roles.	Infrastructure	User Roles	R1C2 Must
RD-8	The system shall support the assignment of one or more roles to a user.	Infrastructure	User Roles	R1C2 Must
RD-864	The system shall not allow critical transaction files to be adjusted by any unauthorized party.	Infrastructure	User Roles	R1C2 Must
RD-9	The system shall support the management of the functions permitted by a user role.	Infrastructure	User Roles	R1C2 Must
RD-1067	The system shall provide the capability for authorized users to define workflows.	Infrastructure	Workflow Management	R1C2 Must
RD-1068	The workflow definition shall be in the XML form conforming to a well established schema, such as XML Process Definition Language (XPDL) of Workflow Management Coalition (WfMC) or the Business Process Execution Language (BPEL) schema.	Infrastructure	Workflow Management	R1C2 Must
RD-1069	The system shall provide the capability for authorized users to validate workflow definitions against the established schema.	Infrastructure	Workflow Management	R1C2 Must
RD-1070	The system shall provide the capability for authorized users to create new versions of workflow definitions.	Infrastructure	Workflow Management	R1C2 Must
RD-1071	The system shall provide the capability for authorized users to test new versions of workflow definitions without interfering with any existing workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1072	The system shall provide the capability for authorized users to place new versions of workflow definitions into production.	Infrastructure	Workflow Management	R1C2 Must
RD-1073	The system shall provide the capability for authorized users to deploy newly developed or modified workflow definitions without interfering with existing workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1075	The system shall provide the capability for authorized users to revert to previous workflow definitions without interfering with existing workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1076	The system shall provide the capability for authorized users to revert to previous workflow definitions without interfering with other non-completed instances of workflows.	Infrastructure	Workflow Management	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1077	The system shall provide the capability for authorized users to manage business rules.	Infrastructure	Workflow Management	R1C2 Must
RD-1078	The workflow-related business rules shall be configurable by authorized users to control the order in which the rules are applied.	Infrastructure	Workflow Management	R2 Must
RD-1079	The system shall provide the capability for authorized users to manage manual activities.	Infrastructure	Workflow Management	R1C2 Must
RD-1080	The system shall provide the capability for authorized users to manage automated activities.	Infrastructure	Workflow Management	R2 Must
RD-1082	The system shall provide the capability for authorized users to append comments on jobs.	Infrastructure	Workflow Management	R1C2 Must
RD-1083	The system shall provide the capability for authorized users to append comments on activities.	Infrastructure	Workflow Management	R1C2 Must
RD-1084	The system shall provide the capability for authorized users to append comments on workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1091	The system shall store information related to workflows in BPI.	Infrastructure	Workflow Management	R1C2 Must
RD-1092	The system shall store information about workflows in BPI.	Infrastructure	Workflow Management	R1C2 Must
RD-1093	The system shall store information about jobs in BPI.	Infrastructure	Workflow Management	R1C2 Must
RD-1094	The system shall store information about activities in BPI.	Infrastructure	Workflow Management	R1C2 Must
RD-1096	The system shall provide the capability for authorized users to control the execution of workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1097	The system shall provide the capability for authorized users to assign priorities to workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1098	The system shall provide the capability for authorized users to schedule for manual and automated activities.	Infrastructure	Workflow Management	R1C2 Must
RD-1100	The system shall provide the capability for authorized users to assign deadlines for jobs.	Infrastructure	Workflow Management	R1C2 Must
RD-1101	The system shall provide the capability for authorized users to assign deadlines for activities.	Infrastructure	Workflow Management	R1C2 Must
RD-1103	The system shall provide the capability for authorized users to assign estimated completion times for jobs.	Infrastructure	Workflow Management	R1C2 Must
RD-1104	The system shall provide the capability for authorized users to assign estimated completion times for activities.	Infrastructure	Workflow Management	R1C2 Must
RD-1105	The system shall provide the capability for authorized users to assign human resources to manual activities.	Infrastructure	Workflow Management	R1C2 Must
RD-1107	The system shall provide the capability for authorized users to suspend activities.	Infrastructure	Workflow Management	R1C2 Must
RD-1108	The system shall provide the capability for authorized users to suspend workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1110	The system shall provide the capability for authorized users to resume activities.	Infrastructure	Workflow Management	R1C2 Must
RD-1111	The system shall provide the capability for authorized users to resume workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1113	The system shall provide the capability for authorized users to cancel activities.	Infrastructure	Workflow Management	R1C2 Must
RD-1114	The system shall provide the capability for authorized users to cancel workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1115	The system shall provide the capability to log activities.	Infrastructure	Workflow Management	R1C2 Must
RD-1116	The system shall provide the capability to log activity start time.	Infrastructure	Workflow Management	R1C2 Must
RD-1117	The system shall provide the capability to log activity end time.	Infrastructure	Workflow Management	R1C2 Must
RD-1118	The system shall provide the capability to log the person(s) performing the activity.	Infrastructure	Workflow Management	R1C2 Must
RD-1119	The system shall provide the capability to log the resources associated with an activity .	Infrastructure	Workflow Management	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1120	The system shall provide the capability for authorized users to manage lists of workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1121	The system shall provide the capability for authorized users to view lists of workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1122	The system shall provide the capability for authorized users to assign lists of workflow instances to other users.	Infrastructure	Workflow Management	R1C2 Must
RD-1123	The system shall provide the capability for authorized users to perform actions on a batch of workflow instances.	Infrastructure	Workflow Management	R2 Must
RD-1124	The system shall provide the capability for authorized users to control the execution of jobs.	Infrastructure	Workflow Management	R1C2 Must
RD-1125	The system shall provide the capability for authorized users to assign priorities to jobs.	Infrastructure	Workflow Management	R1C2 Must
RD-1126	The priority of a job shall be inherited by workflow instances associated with the job.	Infrastructure	Workflow Management	R1C2 Must
RD-1128	The system shall provide the capability for authorized users to suspend jobs.	Infrastructure	Workflow Management	R1C2 Must
RD-1129	The system shall provide the capability for authorized users to resume jobs.	Infrastructure	Workflow Management	R1C2 Must
RD-1130	The system shall provide the capability for authorized users to cancel a job.	Infrastructure	Workflow Management	R1C2 Must
RD-1131	The system shall provide the capability for authorized users to adjust the priority of a job at any time.	Infrastructure	Workflow Management	R2 Must
RD-1132	The system shall provide the capability for authorized users to adjust the priority of a job manually or automatically.	Infrastructure	Workflow Management	R2 Must
RD-1133	The system shall provide the capability to log jobs.	Infrastructure	Workflow Management	R1C2 Must
RD-1134	The system shall provide the capability for authorized users to manage work lists of jobs.	Infrastructure	Workflow Management	R1C2 Must
RD-1135	The system shall provide the capability for authorized users to perform actions on a batch of jobs.	Infrastructure	Workflow Management	R2 Must
RD-1137	The system shall provide a workflow monitoring tool for all workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1138	The workflow monitoring tool shall provide the capability for authorized users to see how many instances of a workflow exist as well as the status of the workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1139	The workflow monitoring tool shall provide the capability for authorized users to see how many instances of a workflow exist.	Infrastructure	Workflow Management	R1C2 Must
RD-1140	The workflow monitoring tool shall provide the capability for authorized users to see the status of the workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1141	The workflow monitoring tool shall provide the capability for authorized users to customize views.	Infrastructure	Workflow Management	R1C2 Must
RD-1142	The workflow monitoring tool shall provide the capability for authorized users to save customized views for future use.	Infrastructure	Workflow Management	R1C2 Must
RD-1143	The workflow monitoring tool shall provide the capability for authorized users to monitor processing history of workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1144	The workflow monitoring tool shall provide the capability for authorized users to monitor processing history over a specified time period.	Infrastructure	Workflow Management	R1C2 Must
RD-1146	The workflow monitoring tool shall report the throughput for workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1147	The workflow monitoring tool shall report any delays for workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1148	The workflow monitoring tool shall report the loads for workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1149	The workflow monitoring tool shall report additional performance measures in the future.	Infrastructure	Workflow Management	R2 Must
RD-1151	The system shall provide the capability for authorized users to monitor jobs.	Infrastructure	Workflow Management	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1152	The system shall provide the capability for authorized users to monitor a list of jobs.	Infrastructure	Workflow Management	R1C2 Must
RD-1153	The system shall provide the capability for authorized users to monitor a batch of jobs.	Infrastructure	Workflow Management	R1C2 Must
RD-1155	The system shall provide the capability for authorized users to monitor planned times for selected jobs.	Infrastructure	Workflow Management	R2 Must
RD-1156	The system shall provide the capability for authorized users to monitor scheduled times for selected jobs.	Infrastructure	Workflow Management	R2 Must
RD-1157	The system shall provide the capability for authorized users to monitor actual times for selected jobs.	Infrastructure	Workflow Management	R2 Must
RD-1158	The system shall provide the capability for authorized users to group jobs with a defined status.	Infrastructure	Workflow Management	R1C2 Must
RD-1160	The system shall provide the capability for authorized users to monitor workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1161	The system shall provide the capability for authorized users to monitor workflow instances or a list of workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1162	The system shall provide the capability for authorized users to monitor a batch of workflow instances.	Infrastructure	Workflow Management	R1C2 Must
RD-1164	The system shall provide the capability for authorized users to monitor planned times for selected workflow instances.	Infrastructure	Workflow Management	R2 Must
RD-1165	The system shall provide the capability for authorized users to monitor scheduled times for selected workflow instances.	Infrastructure	Workflow Management	R2 Must
RD-1166	The system shall provide the capability for authorized users to monitor actual times for selected workflow instances.	Infrastructure	Workflow Management	R2 Must
RD-1167	The system shall provide the capability to sort workflow instances with a defined status.	Infrastructure	Workflow Management	R2 Must
RD-1169	The system shall provide the capability to estimate resource requirements associated with internal workflow.	Infrastructure	Workflow Management	R1C2 Must
RD-1170	The system shall provide the capability to estimate resource requirements associated with external workflow.	Infrastructure	Workflow Management	R1C2 Could / R2 Must
RD-1172	The system shall provide the capability to estimate resource requirements for automated activities.	Infrastructure	Workflow Management	R1C2 Could / R2 Must
RD-1173	The system shall provide the capability to estimate resource requirements for manual activities.	Infrastructure	Workflow Management	R1C2 Could / R2 Must
RD-1175	The system shall provide the capability to associate notifications with workflows.	Infrastructure	Workflow Management	R1C2 Must
RD-1176	The system shall provide the capability to manage notifications associated with workflows.	Infrastructure	Workflow Management	R1C2 Must
RD-1178	The system shall send workflow notifications via e-mail.	Infrastructure	Workflow Management	R1C2 Must
RD-1179	The system shall send workflow alerts via the user's screen.	Infrastructure	Workflow Management	R1C2 Must
RD-1180	The system shall send workflow notifications via additional methods in the future.	Infrastructure	Workflow Management	R2 Must
RD-1181	The system shall provide the capability for authorized users to configure the list of recipients of workflow notifications and alerts.	Infrastructure	Workflow Management	R1C2 Must
RD-1182	The system shall provide the capability for authorized users to escalate workflow notifications.	Infrastructure	Workflow Management	R3 Should
RD-1184	The system shall provide the capability for authorized users to have security controls on workflow activities.	Infrastructure	Workflow Management	R1C2 Must
RD-1185	The security control (allow or deny actions) for workflow shall be rule based.	Infrastructure	Workflow Management	R2 Must
RD-1186	Manual activities in the workflows shall be assigned with one or more security rules.	Infrastructure	Workflow Management	R2 Must
RD-1188	The system shall provide a Graphical User Interface (GUI) edit tool to manage workflow definitions and executions.	Infrastructure	Workflow Management	R1C2 Must
RD-1189	The Monitoring Tool shall contain a GUI for all workflow monitoring capabilities.	Infrastructure	Workflow Management	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-14	The system shall support the capability to accommodate changes in processes without requiring major reengineering or design changes.	Infrastructure	Workflow Management	R1C2 Must
RD-15	The system shall support the capability to accommodate changes in policies without requiring major reengineering or design changes.	Infrastructure	Workflow Management	R1C2 Must
RD-3026	The system shall provide the capability to configure workbenches according to criticality and release schedules specified in individual requirements.	Infrastructure	Workflow Management	R2 Must
RD-3565	The system shall have the capability to assign human resources to manual activities.	Infrastructure	Workflow Management	R1C2 Must

3.7 METADATA MANAGEMENT FEATURE GROUP REQUIREMENTS

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1000	The system shall provide the capability to include non-repudiation information in metadata.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-1001	Non-repudiation metadata shall have the capability to include the sender's identity and proof.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-1002	Non-repudiation metadata shall have the capability to include the recipient's identity and proof.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-1004	Intended Use metadata shall have the capability to identify the content delivery method designated by an authorized user that must be used for the purpose of citation in court.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-1005	Intended Use metadata shall have the capability to identify the file format designated by an authorized user that must be used for the purpose of citation in court	Metadata Management	Authenticity Metadata	R1C4 Must
RD-1006	Intended Use metadata shall have the capability to identify the content presentation designated by an authorized user that must be used for the purpose of citation in court.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-302	The AIP shall include preservation metadata to record events and preservation processes, from ingest into the repository throughout its lifecycle.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-318	The system shall have the capability to include source metadata about converted content.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-3883	The system shall record in each history the unique identifier of the digital object affected by the event.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3884	The system shall assign an identifier to each type of event the system will record in history entries.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3885	The system shall record a history entry for every system action that adds, modifies, or deletes metadata in the package, excluding changes to events metadata.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3887	The system shall record a history entry for every step in the ingest processing of a package.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3888	The system shall record history entries in a package's PREMIS metadata for each significant event in the life of a package.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3889	The system shall record history entries according to the PREMIS data dictionary.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3890	The system shall record history entries according to the PREMIS events and agents schemas v. 1.0.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3891	The system shall record a history entry for every system action that adds or deletes a content file in the package.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3892	The system shall record a history entry for any integrity check.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3893	The system shall record the event type in each history entry.	Metadata Management	Authenticity Metadata	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3894	The system shall record the identifier for the type of event in each history entry.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3895	In each history entry, the system shall record the time and date of the event occurrence in ISO 8601 format.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3896	The system shall record in each history the outcome of the event.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3897	The system shall record in each history a categorization of the outcome of the event in terms of success, partial success, or failure.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3898	The system shall record in each history the identification of the agents associated with the event.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3899	The system shall record in each history the role of the agents associated with the event.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3900	The system shall assign an identifier to each agent in the system that is capable of authorizing, implementing, validating or executing an event in history entries.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3901	The system shall maintain a human-readable table of identifiers for all agents in the system and the associated user name or software process.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3902	The system shall allow authorized users to view the table of agent identifiers and the associated user name or software process.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3903	Event type identifiers shall be unique to each event type.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3904	Agent identifiers shall be unique to each agent.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3905	Event type identifiers shall not be reused.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3906	Agent identifiers shall not be reused.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3907	The system shall make available provenance information to all users.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-3908	The system shall have the capability to restrict the view of some event types and agents to authorized users.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-777	The system shall provide the capability for authorized users to record information about the intended use in the metadata.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-800	The system shall have the capability to record intended use in metadata.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-826	The system shall have the capability to record intended use in metadata.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-829	The system shall provide the capability to recognize integrity marks at pre-ingest.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-830	The system shall provide the capability to validate integrity marks at pre-ingest.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-833	Where public key cryptography and digital certificates are used to create a digital signature integrity mark on content that is submitted to GPO for ingest into the system, the system shall record in metadata that a digital signature was present.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-834	Where public key cryptography and digital certificates are used to create a digital signature integrity mark on content that is submitted to GPO for ingest into the system, the system shall make metadata information concerning the presence of a digital signature available to End Users.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-838	The system shall have the capability to gather relevant information from integrity marks (e.g., digital signatures, digital certificates) for use as part of the chain of custody.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-839	The system shall have the ability to gather Distinguished Name information from integrity marks for use as part of the chain of custody.	Metadata Management	Authenticity Metadata	R1C4 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-840	The system shall have the capability to gather information from integrity marks regarding the date the integrity mark was applied for use as part of the chain of custody.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-841	The system shall have the capability to gather information from integrity marks regarding the time the integrity mark was applied for use as part of the chain of custody.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-842	The system shall have the capability to record chain of custody in WIP.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-856	The system shall comply with the technical requirements of Trustworthy Repositories Audit & Certification (TRAC): Criteria and Checklist.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-857	The system shall provide the capability to certify content integrity within the system by ensuring that content has not been altered in an unauthorized manner.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-858	The system shall provide the capability to certify content integrity within the system by ensuring that content has not been destroyed in an unauthorized manner.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-871	The system shall have the capability to validate a cryptographic digital signature, in accordance with IETF RFC 3447 on content in pre-ingest, to ensure that the content has not been altered, and that the signer's certificate is valid before ingesting the content.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-989	Authenticity metadata shall have the capability to include the source of deposited, harvested, and converted content.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-990	Authenticity metadata shall have the capability to include identity of the submitter and the identify of the user who approved content for publication.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-991	Authenticity metadata shall have the capability to include the source of tangible content that was used to create converted content.	Metadata Management	Authenticity Metadata	R1C4 Must
RD-992	Authenticity metadata shall have the capability to include the chain of custody information about content from the producer to the archive.	Metadata Management	Authenticity Metadata	R1C2 Must
RD-994	Integrity metadata shall have the capability to include information about any ingest integrity checks	Metadata Management	Authenticity Metadata	R1C2 Must
RD-136	The system shall have the capability to automatically record in BPI information about the actions performed by business processes on content.	Metadata Management	Content Metadata	R1C2 Must
RD-137	The system shall record all additions, deletions, and changes to content metadata within the system.	Metadata Management	Content Metadata	R1C2 Must
RD-1807	The system shall accept all administrative and descriptive metadata supplied by the submission agency/authority.	Metadata Management	Content Metadata	R1C4 Must
RD-1817	The system shall provide the capability to record Rights Owner of the content.	Metadata Management	Content Metadata	R1C4 Must
RD-1823	The system shall provide the capability to record Intended Output of the content.	Metadata Management	Content Metadata	R1C4 Must
RD-1824	The system shall provide the capability to record Intended Audience of the content.	Metadata Management	Content Metadata	R1C4 Must
RD-2885	The system shall provide capability for authorized users to add metadata.	Metadata Management	Content Metadata	R1C2 Must
RD-2886	The system shall provide capability for authorized users to modify metadata.	Metadata Management	Content Metadata	R1C2 Must
RD-2887	The system shall provide capability for authorized users to delete metadata.	Metadata Management	Content Metadata	R1C2 Must
RD-3909	The system shall transform metadata to user-friendly values for display on the content detail page, according to the Content Detail Display Specification.	Metadata Management	Content Metadata	R1C2 Must
RD-45	The system shall reflect changes to AIP metadata in the ACP and vice versa.	Metadata Management	Content Metadata	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-50	The system shall have the capability to employ multiple content metadata schema, and to process and preserve multiple sets of content metadata for a digital object.	Metadata Management	Content Metadata	R1C2 Must
RD-53	The system shall provide the capability to link content metadata with system metadata.	Metadata Management	Content Metadata	R1C2 Must
RD-54	The system shall provide the capability to link content metadata with business process information.	Metadata Management	Content Metadata	R1C2 Must
RD-1808	The system shall provide the capability to record Title or caption of content.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-1810	The system shall provide the capability to record the Persistent names assigned to content.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-1812	The system shall provide the capability to record the ISBN/ISSNs assigned to content.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-1815	The system shall provide the capability to record Author/Creator of the content.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-1816	The system shall provide the capability to record Publisher/Authority of the content.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-1821	The system shall provide the capability to record content description information.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-1900	The system shall record the language of the publication.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-217	The system shall allow all MODS elements to be stored in the MODS file in content packages.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-218	The system shall allow all MODS sub-elements to be stored in the MODS file in content packages.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-2874	The system shall apply authority control to certain fields to provide cross-referencing of terms.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-2879	The system shall support the extraction of metadata from content.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-2881	The system shall provide for the creation of new metadata records based on existing metadata records.	Metadata Management	Descriptive Metadata	R1C4 Must
RD-2883	The system shall relate descriptive metadata with the content described.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-2889	The system shall have the ability to provide access to metadata throughout the lifecycle of the content.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-2937	The system shall support the creation of ONIX records.	Metadata Management	Descriptive Metadata	R1C4 Must
RD-2970	The system shall support non web-based GUIs, as necessary.	Metadata Management	Descriptive Metadata	R1C2 Should
RD-3538	Metadata associated with each rendition in a package shall have the capability to indicate whether the rendition is one or more of the following: screen optimized, print optimized, press optimized, native, highest fidelity	Metadata Management	Descriptive Metadata	R1C2 Must
RD-363	The system shall have the capability to use descriptive metadata extension schema to support access to publications.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3910	The DIP shall have the capability to contain metadata indicating if the publication it contains is in scope for GPO's dissemination programs.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3911	The system shall enforce a controlled vocabulary for selected metadata elements as defined by each schemas implementation technical memo when a user modifies content metadata.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3912	The system shall enforce a controlled vocabulary for selected metadata elements as defined by each schemas implementation technical memo when content metadata is submitted to the system.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3913	The system shall enforce a controlled vocabulary for selected metadata elements as defined by each schemas implementation technical memo when content is metadata created by the system.	Metadata Management	Descriptive Metadata	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3914	The system shall validate metadata against its schema after any change to the metadata.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3915	The system shall validate that metadata meets the implementation technical memo for the schema after any change to the metadata.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3916	The system shall allow authorized users to add content metadata using a graphical user interface.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3917	The system shall allow authorized users to modify content metadata using a graphical user interface.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3918	The system shall allow authorized users to delete content metadata using a graphical user interface.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3919	The system shall determine and record content metadata for documents in GPO Access Collections as referenced in RD-2596.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3920	The system shall analyze content to determine and record granule-specific metadata for well formed publications.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3921	The system shall analyze content to determine and record publication-specific metadata for well formed publications.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3922	The system shall determine and record content metadata for granules in GPO Access Collections as referenced in RD-2596.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3923	The system shall analyze content to determine and record granule-specific metadata to specifications.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3924	The system shall provide an interface for authorized users for performing batch text string search and replacement in a selected metadata field.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3925	The system shall require a user confirmation before making each change in a metadata search and replacement operation.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3926	The system shall include the user-relative location (full URL) for the digital object, where PURL is not available in the MODS descriptive metadata element location:url.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3927	The system shall include the user-relative location (full URL) for the objects in the internal ACP in the MODS descriptive metadata element location:url.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3928	The system shall include the persistent name of the digital object, where available in the MODS descriptive metadata element location:url.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-3929	The system shall analyze content to determine and record metadata specific to select publications enumerated in RD-2596 (list of GPO Access Collections in MODS,	Metadata Management	Descriptive Metadata	R1C2 Must
RD-62	The system shall employ publication-specific metadata as required to support existing publications.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-63	The system shall employ granule-specific metadata as required to support existing publications	Metadata Management	Descriptive Metadata	R1C2 Must
RD-68	The system shall record the context of a digital object and relationship to other objects in metadata.	Metadata Management	Descriptive Metadata	R1C4 Must
RD-764	The system shall record persistent names associated with content.	Metadata Management	Descriptive Metadata	R1C4 Must
RD-765	The system shall record existing persistent names associated with content.	Metadata Management	Descriptive Metadata	R1C2 Must
RD-816	The source of converted content shall be recorded in metadata.	Metadata Management	Descriptive Metadata	R1C4 Must
RD-2873	The system shall exclude issues in known series and serials from records from being sent to the ILS	Metadata Management	ILS Integration	R1C2 Must
RD-2878	The system shall maintain a dynamic list of series and serials from information in the ILS.	Metadata Management	ILS Integration	R1C4 Must
RD-2893	Upon ingest of a package, the system shall send a preliminary acquisitions record in MARC format to the ILS	Metadata Management	ILS Integration	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2941	When changes are made to a bibliographic record in the ILS, the system shall incorporate the changes to the appropriate content package or content packages	Metadata Management	ILS Integration	R1C2 Must
RD-2943	When a new bibliographic record is created in the ILS, the system shall save the record as MARCXML in the content package	Metadata Management	ILS Integration	R1C2 Must
RD-2944	When a bibliographic record is deleted in the ILS, the system shall delete the ACP, subject to approval by an authorized user	Metadata Management	ILS Integration	R1C2 Must
RD-2945	When the system creates a new MARCXML from a bibliographic record from the ILS, the system shall update the MARCXML with the appropriate FDsys unique IDs	Metadata Management	ILS Integration	R1C2 Must
RD-2948	The system shall send a notification to an authorized user that a new item in a series or serial is available	Metadata Management	ILS Integration	R1C2 Must
RD-2950	When changes are made to a bibliographic record in the ILS, the system shall incorporate the changes to the MODS record of the appropriate content package or content packages	Metadata Management	ILS Integration	R1C2 Must
RD-3932	The system shall exclude records from being sent to the ILS based on a set of configurable criteria.	Metadata Management	ILS Integration	R2 Must
RD-3934	The system shall maintain a dynamic list of serials and series based on cataloging records from the ILS.	Metadata Management	ILS Integration	R2 Must
RD-298	For each rendition in a content package there shall be a corresponding metadata file specifying technical parameters of the content file.	Metadata Management	Mandatory AIP Metadata	R1C2 Must
RD-3522	A AIP that describes a publication which only exists in tangible form shall contain a surrogate digital object that describes its tangible expression.	Metadata Management	Mandatory AIP Metadata	R1C4 Must
RD-3523	The AIP shall contain a descriptive metadata file for the package in MODS format.	Metadata Management	Mandatory AIP Metadata	R1C2 Must
RD-3525	The URL of harvest descriptive metadata element is mandatory for AIPs that are harvested content	Metadata Management	Mandatory AIP Metadata	R1C4 Must
RD-3527	The physicalLocation descriptive metadata element is mandatory for AIPs where the content exists only in tangible form.	Metadata Management	Mandatory AIP Metadata	R1C4 Must
RD-3528	The date of capture descriptive metadata element is mandatory for AIPs that are harvested content	Metadata Management	Mandatory AIP Metadata	R1C4 Must
RD-3529	The descriptive metadata source metadata element is mandatory for AIPs.	Metadata Management	Mandatory AIP Metadata	R1C2 Must
RD-3530	The descriptive metadata date of creation metadata element is mandatory for AIPs.	Metadata Management	Mandatory AIP Metadata	R1C2 Must
RD-3531	The date of ingest descriptive metadata element is mandatory for AIPs	Metadata Management	Mandatory AIP Metadata	R1C2 Must
RD-3532	The FDsys content package unique ID metadata element is mandatory for AIPs.	Metadata Management	Mandatory AIP Metadata	R1C2 Must
RD-3533	The MIME type metadata element for each file is mandatory for AIPs.	Metadata Management	Mandatory AIP Metadata	R1C2 Must
RD-3534	The file size metadata element for each file is mandatory for AIPs	Metadata Management	Mandatory AIP Metadata	R1C2 Must
RD-3535	The agency publisher descriptive metadata element is mandatory for AIPs	Metadata Management	Mandatory AIP Metadata	R1C2 Must
RD-3536	A descriptive metadata element indicating that the content is in scope for GPO's dissemination program shall be considered mandatory for AIPs.	Metadata Management	Mandatory AIP Metadata	R1C2 Must
RD-3537	The title descriptive metadata element is mandatory for AIPs.	Metadata Management	Mandatory AIP Metadata	R1C2 Must
RD-817	The source of tangible content that was used to create the converted content shall be recorded in metadata. (e.g., OriginInfo:publisher)	Metadata Management	Mandatory AIP Metadata	R1C4 Must
RD-153	The SIP shall have the capability to contain metadata indicating if the publication it contains is in scope for GPO's dissemination programs.	Metadata Management	Mandatory SIP Metadata	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-197	The SIP shall contain a descriptive metadata file for the package in MODS format.	Metadata Management	Mandatory SIP Metadata	R1C2 Must
RD-220	The agency publisher descriptive metadata element shall be mandatory for SIPs	Metadata Management	Mandatory SIP Metadata	R1C2 Must
RD-229	The descriptive metadata source metadata element is mandatory for SIPs.	Metadata Management	Mandatory SIP Metadata	R1C2 Must
RD-3517	The location:physicalLocation MODS descriptive metadata element shall be considered mandatory for SIPs where the content exists only in tangible form.	Metadata Management	Mandatory SIP Metadata	R1C4 Must
RD-3518	The location:url MODS descriptive metadata element shall be considered mandatory for SIPs that are harvested content	Metadata Management	Mandatory SIP Metadata	R1C4 Must
RD-3519	The originInfo:dateCaptured MODS descriptive metadata element shall be considered mandatory for SIPs that are harvested content	Metadata Management	Mandatory SIP Metadata	R1C4 Must
RD-3520	The descriptive metadata date of creation metadata element is mandatory for SIPs.	Metadata Management	Mandatory SIP Metadata	R1C2 Must
RD-1796	The system shall have the capability to allow authorized users to modify access rights to content based on copyright information provided by Content Originators.	Metadata Management	Rights Metadata	R1C4 Must
RD-1798	Copyright information will be recorded in metadata.	Metadata Management	Rights Metadata	R1C4 Must
RD-378	The system shall have the capability to include rights metadata about each rendition in the ACP.	Metadata Management	Rights Metadata	R1C4 Must
RD-64	The system shall employ metadata which relates the rights information of a target digital object(s) and its associated content package.	Metadata Management	Rights Metadata	R1C4 Must
RD-96	The system shall provide the capability to add new versions of XML schema to the Schema Registry.	Metadata Management	Schema Registry	R1C4 Must
RD-99	The system shall provide the capability to add new XML DTDs to the Schema Registry.	Metadata Management	Schema Registry	R1C4 Must
RD-103	Any schema registered in FDsys shall act as an extension schema to METS	Metadata Management	Schema Registry	R1C2 Must
RD-104	The schema shall map to specific function(s), content type, or content formats within the system.	Metadata Management	Schema Registry	R1C4 Must
RD-110	The system shall provide the capability to add extension schema developed by GPO to the Schema Registry.	Metadata Management	Schema Registry	R1C4 Must
RD-111	Specific schema for each digital object shall be based on the specific needs of the target digital object or content package.	Metadata Management	Schema Registry	R1C4 Must
RD-132	The system shall provide the capability to transform metadata from one extension schema to another.	Metadata Management	Schema Registry	R1C4 Must
RD-216	The system shall employ MODS XML schema version 3.2 in content packages.	Metadata Management	Schema Registry	R1C2 Must
RD-313	Each metadata file in the content package shall identify which METS extension schema it conforms to.	Metadata Management	Schema Registry	R1C2 Must
RD-3507	The system shall have the capability to store metadata in any registered input standard in the SIP.	Metadata Management	Schema Registry	R1C2 Must
RD-3510	The system shall have the capability to store metadata in any registered extension schema in a content package.	Metadata Management	Schema Registry	R1C2 Must
RD-3513	The system shall have the capability to employ Dublin Core that is not expressed in XML as an input standard.	Metadata Management	Schema Registry	R1C4 Must
RD-3514	The system shall provide the capability to add new input standards to the Schema Registry.	Metadata Management	Schema Registry	R1C4 Must
RD-3936	The system shall have the capability to employ MARC 21 XML schema as an extension schema.	Metadata Management	Schema Registry	R1C2 Must
RD-3937	The system shall have the capability to store metadata in any registered input standard in the DIP.	Metadata Management	Schema Registry	R1C2 Must
RD-437	The system shall have the capability to read registered metadata schema to extract metadata for use by the system.	Metadata Management	Schema Registry	R1C2 Must
RD-51	The system shall have the capability to deliver a full metadata record in a requested schema regardless of the schema the metadata is stored in the content package.	Metadata Management	Schema Registry	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-57	All metadata files shall be encoded in XML and conform to schema that are adopted by FDsys.	Metadata Management	Schema Registry	R1C2 Must
RD-75	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata.	Metadata Management	Schema Registry	R1C2 Must
RD-78	The system shall have the capability to employ Dublin Core version 1.1 expressed in XML as an extension schema.	Metadata Management	Schema Registry	R1C4 Must
RD-80	The system shall have the capability to employ Machine Readable Cataloging (MARC21) as an input standard.	Metadata Management	Schema Registry	R1C2 Must
RD-81	The system shall have the capability to employ Metadata Object Description Schema (MODS) version 3.2 as an extension schema.	Metadata Management	Schema Registry	R1C2 Must
RD-91	The system shall have the capability to employ MIX (NISO Metadata for Images) as an extension schema.	Metadata Management	Schema Registry	R1C4 Must
RD-94	The system shall provide the capability to add new XML schema to the Schema Registry.	Metadata Management	Schema Registry	R1C4 Must
RD-97	The system shall provide the capability to add new versions of XML DTDs to the Schema Registry.	Metadata Management	Schema Registry	R1C4 Must
RD-77	The system shall support the capability to translate metadata conforming to registered input standards to a registered extension schema for storage in the system.	Metadata Management	Schema Registry	R1C2 Must
RD-149	The metadata for converted content in the SIP shall support the inclusion of full technical information on the conversion as specified by NISO Z 39.87-2006	Metadata Management	Technical Metadata	R1C4 Must
RD-1791	The system shall identify files with security restrictions upon submission.	Metadata Management	Technical Metadata	R1C4 Must
RD-1811	The system shall provide the capability to record the filenames assigned to content.	Metadata Management	Technical Metadata	R1C2 Must
RD-1829	The system shall ascertain the software applications and versions used to create the digital objects, where possible.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1830	The system shall ascertain the page size of the publication.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1831	The system shall ascertain the trim size of the publication.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1832	The system shall ascertain the number of pages.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1834	The system shall ascertain file sizes.	Metadata Management	Technical Metadata	R1C2 Must
RD-1835	The system shall ascertain what fonts are used in the publication.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1836	The system shall ascertain if the fonts are furnished or embedded.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1837	The system shall ascertain font types.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1838	The system shall ascertain what color mode(s) are used in the publication.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1839	The system shall ascertain whether bleed is required/provided for.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1840	The system shall ascertain information about the construction of a publication.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1841	The system shall ascertain image resolutions.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1842	The system shall ascertain the language of the publication.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1843	The system shall ascertain file compression information.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1846	The system shall ascertain audio playing time.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1847	The system shall ascertain the language of audio.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1848	The system shall ascertain audio file compression information.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1849	The system shall support the capability to ascertain the bit rate of audio.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1852	The system shall ascertain closed captioning information.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1853	The system shall ascertain video runtime.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1854	The system shall ascertain video encoding scheme.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1855	The system shall ascertain the language of the video.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1856	The system shall ascertain video file compression information.	Metadata Management	Technical Metadata	R1C4 Should / R2 Must
RD-1901	The system shall record file compression information.	Metadata Management	Technical Metadata	R1C4 Must
RD-259	The AIP shall contain Representation Information metadata for every rendition of the publication in the AIP.	Metadata Management	Technical Metadata	R1C2 Must
RD-311	The AIP shall include metadata that expresses Preservation Description Information (PDI) according to the PREMIS schemas.	Metadata Management	Technical Metadata	R1C2 Must
RD-3521	The system shall have the capability to store administrative metadata in PREMIS format in content packages	Metadata Management	Technical Metadata	R1C2 Must
RD-3541	The system shall allow users to view technical metadata included with a digital still image	Metadata Management	Technical Metadata	R1C4 Must
RD-3542	The system shall allow users to view technical metadata imbedded in a digital still image	Metadata Management	Technical Metadata	R1C4 Must
RD-3580	The system shall copy last modification date to technical metadata where it exists.	Metadata Management	Technical Metadata	R1C4 Must
RD-3581	The system shall copy an objects byte size to technical metadata.	Metadata Management	Technical Metadata	R1C2 Must
RD-3582	The system shall copy an objects file pathname or URL to technical metadata.	Metadata Management	Technical Metadata	R1C2 Must
RD-3938	The system will define significant properties for preservation, as defined by the PREMIS data dictionary.	Metadata Management	Technical Metadata	R1C2 Must
RD-3939	The system shall ascertain, where possible, and record technical metadata for each object, according to the PREMIS data dictionary.	Metadata Management	Technical Metadata	R1C2 Must
RD-643	The system shall use the PREMIS Preservation Metadata Schema version 1.0 as an extension schema.	Metadata Management	Technical Metadata	R1C2 Must
RD-1013	The system shall allow an authorized user to manage the order of versions.	Metadata Management	Version Control	R1C2 Must
RD-1015	The system shall allow authorized users to input version information.	Metadata Management	Version Control	R1C4 Must
RD-1016	The system shall allow authorized users to view version information.	Metadata Management	Version Control	R1C4 Must
RD-1017	The system shall allow authorized users to manage version information.	Metadata Management	Version Control	R1C4 Must
RD-1050	The system shall express version information in metadata.	Metadata Management	Version Control	R1C2 Must
RD-1820	The system shall provide the capability to record superseded document information (i.e. publication title(s), series number, and stock number(s) of replaced versions).	Metadata Management	Version Control	R1C4 Must
RD-2847	The system shall provide the capability for users to navigate to other versions of the content.	Metadata Management	Version Control	R1C2 Must
RD-2891	The system shall record the relationships among the issues or volumes of serially-issued publications.	Metadata Management	Version Control	R1C2 Must
RD-3941	The system shall express superseding publication information in the metadata.	Metadata Management	Version Control	R1C2 Must
RD-3942	The system shall express star print information in the metadata.	Metadata Management	Version Control	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3943	The system shall delete an ACP in the case that the content has been replaced by a star print version.	Metadata Management	Version Control	R1C2 Must
RD-3944	The system shall have the capability to record unique IDs of related versions in the metadata.	Metadata Management	Version Control	R1C2 Must
RD-3945	The system shall express serial or series information in metadata.	Metadata Management	Version Control	R1C2 Must
RD-3946	The system shall provide the capability to record the order of issues in a serial.	Metadata Management	Version Control	R1C2 Must
RD-3947	The system shall provide the capability to record the order of volumes in a series.	Metadata Management	Version Control	R1C2 Must
RD-3948	The system shall provide the capability to record issue or volume information of the publication.	Metadata Management	Version Control	R1C2 Must
RD-3949	The system shall provide the capability to record the repeated or predictable pattern of a serial.	Metadata Management	Version Control	R1C2 Must
RD-3950	The system shall provide the capability to record the structure of a series.	Metadata Management	Version Control	R1C4 Must
RD-3951	The system shall provide the capability to record the structure of a serial.	Metadata Management	Version Control	R1C4 Must
RD-3952	The system shall provide the capability for users to navigate to other issues or volumes of the publications.	Metadata Management	Version Control	R1C2 Must
RD-3953	The system shall have the capability to record unique IDs of related issues or volumes in the metadata.	Metadata Management	Version Control	R1C2 Must
RD-444	The system shall record the order of versions.	Metadata Management	Version Control	R1C2 Must

3.8 OAIS COMPLIANCE FEATURE GROUP REQUIREMENTS

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2324	The system shall provide the capability to limit access to Sensitive But Unclassified (SBU) content as specified by authorized users.	OAIS Compliance	ACP Creation	R1C4 Must
RD-326	The system shall provide the capability for authorized users to add renditions of a publication to an ACP.	OAIS Compliance	ACP Creation	R1C2 Must
RD-333	The ACP shall have the capability to include publications that are not in scope of GPO's dissemination programs.	OAIS Compliance	ACP Creation	R1C2 Must
RD-338	The ACP shall have the capability to include all content renditions included in its corresponding AIP.	OAIS Compliance	ACP Creation	R1C2 Must
RD-339	The ACP shall contain the descriptive, rights and provenance metadata as exists in the corresponding AIP.	OAIS Compliance	ACP Creation	R1C2 Must
RD-341	The ACP shall have the capability to replicate the structural layout of an AIP.	OAIS Compliance	ACP Creation	R1C2 Must
RD-344	The ACP shall have the capability to be linked to one AIP, known as its corresponding AIP.	OAIS Compliance	ACP Creation	R1C2 Must
RD-345	The ACP shall have the capability to include one or more renditions from its corresponding AIP.	OAIS Compliance	ACP Creation	R1C2 Must
RD-347	The ACP shall have the capability to include copies of all renditions from its corresponding AIP whose metadata indicates they are screen optimized renditions.	OAIS Compliance	ACP Creation	R1C2 Must
RD-348	The ACP shall have the capability to include copies of all renditions from its corresponding AIP whose metadata indicates they are press optimized renditions.	OAIS Compliance	ACP Creation	R1C2 Must
RD-349	The ACP shall have the capability to include copies of all renditions from its corresponding AIP whose metadata indicates they are print optimized renditions.	OAIS Compliance	ACP Creation	R1C2 Must
RD-352	An ACP shall have the capability to contain a METS file named acp.xml.	OAIS Compliance	ACP Creation	R1C2 Must
RD-370	The ACP shall have the capability to include mandatory descriptive metadata elements from the AIP and SIP.	OAIS Compliance	ACP Creation	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3954	The system shall have the capability to create an ACP from an AIP after ingest.	OAIS Compliance	ACP Creation	R1C2 Must
RD-3955	At creation, the ACP shall include all content included in its corresponding AIP except for preservation renditions created by the system during ingest processing.	OAIS Compliance	ACP Creation	R1C2 Must
RD-3956	The system shall have the capability to copy access renditions created during access processing from the ACP to the corresponding AIP.	OAIS Compliance	ACP Creation	R1C2 Must
RD-3957	The system shall indicate in an AIPs provenance metadata that the access rendition was derived during access processing performed on its corresponding ACP.	OAIS Compliance	ACP Creation	R1C2 Must
RD-3958	The system shall provide the capability for authorized users to add renditions of a publication to an AIP.	OAIS Compliance	ACP Creation	R1C2 Must
RD-3959	The ACP shall contain the technical metadata from the corresponding AIP.	OAIS Compliance	ACP Creation	R1C2 Must
RD-485	The system shall create an ACP from the SIP or the AIP.	OAIS Compliance	ACP Creation	R1C2 Must
RD-247	The system shall provide the capability for authorized users to delete renditions of a publication from an AIP.	OAIS Compliance	Delete Packages	R1C2 Must
RD-277	The system shall provide the capability for authorized users to delete AIPs.	OAIS Compliance	Delete Packages	R1C2 Must
RD-278	In order to delete an AIP, two authorized users shall be required to approve the deletion.	OAIS Compliance	Delete Packages	R1C2 Must
RD-327	The ACP shall have the capability to be retained in the system for period of time as is indicated in metadata.	OAIS Compliance	Delete Packages	R1C4 Must
RD-331	The system shall provide the capability for authorized users to delete renditions of a publication from an ACP.	OAIS Compliance	Delete Packages	R1C2 Must
RD-350	The system provide the capability for authorized users to delete entire ACPs.	OAIS Compliance	Delete Packages	R1C2 Must
RD-3960	The system shall apply a digital timestamp to content when new renditions are created.	OAIS Compliance	Digital Time Stamping	R1C2 Must
RD-3961	The system shall apply a digital timestamp when all renditions in a content package are deleted.	OAIS Compliance	Digital Time Stamping	R1C2 Must
RD-468	The system shall apply a digital time stamp to content when content is received.	OAIS Compliance	Digital Time Stamping	R1C2 Must
RD-503	The system shall have the capability to determine whether changes have been made to content.	OAIS Compliance	Digital Time Stamping	R1C2 Must
RD-795	The system shall record information about content integrity in metadata.	OAIS Compliance	Digital Time Stamping	R1C2 Must
RD-849	The system shall apply a digital timestamp to content at ingest.	OAIS Compliance	Digital Time Stamping	R1C2 Must
RD-893	The system shall provide the capability to provide date and time verification.	OAIS Compliance	Digital Time Stamping	R1C2 Must
RD-894	The system time shall be controlled by the network time.	OAIS Compliance	Digital Time Stamping	R1C2 Must
RD-895	The system shall be flexible enough to provide date and time verification through a time certification authority.	OAIS Compliance	Digital Time Stamping	R1C4 Must
RD-896	The system shall be flexible enough to provide date and time verification through a network time server.	OAIS Compliance	Digital Time Stamping	R1C2 Must
RD-897	The system shall be flexible enough to provide date and time verification through the signer's system.	OAIS Compliance	Digital Time Stamping	R1C2 Must
RD-3558	The system shall automatically identify the digital object file format and version.	OAIS Compliance	Format Identification	R1C3 Must
RD-3559	The system shall store digital object file format and version number in technical metadata.	OAIS Compliance	Format Identification	R1C3 Must
RD-3560	The system shall note in technical metadata if it is unable to automatically identify the file format of a digital object.	OAIS Compliance	Format Identification	R1C3 Must
RD-3561	The system shall store an open technical file format registry's unique ID for each digital object's file format in metadata.	OAIS Compliance	Format Identification	R1C3 Must
RD-3562	The system shall store the MIME type of file format in technical metadata.	OAIS Compliance	Format Identification	R1C3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3563	The system shall notify a user that manual identification is necessary if it could not automatically identify the file format.	OAIS Compliance	Format Identification	R1C3 Must
RD-3564	The system shall allow the user to manually change the results of the format identification.	OAIS Compliance	Format Identification	R1C3 Must
RD-3567	The system shall evaluate digital objects for adherence to syntactic requirements for its format	OAIS Compliance	Format Identification	R1C3 Must
RD-3570	The system shall record the reasons for file format validation failure in metadata.	OAIS Compliance	Format Identification	R1C3 Must
RD-3571	The system shall notify users of a failure in file format validation.	OAIS Compliance	Format Identification	R1C3 Must
RD-3572	The system shall allow authorized users to download and manually inspect a digital object that fails file format validation.	OAIS Compliance	Format Identification	R1C3 Must
RD-3573	The system shall allow an authorized user to manually change the results of the file format validation.	OAIS Compliance	Format Identification	R1C3 Must
RD-3576	The system shall allow a user to manually record the function inhibited by a digital object inhibitor	OAIS Compliance	Format Identification	R1C3 Must
RD-3578	The system shall allow users to view technical metadata included with a digital still image as specified by NISO Z39.87	OAIS Compliance	Format Identification	R1C4 Must
RD-3583	The system shall allow a user to manually change the format characterization in the technical metadata.	OAIS Compliance	Format Identification	R1C4 Must
RD-3584	The system shall record characterization errors in technical metadata.	OAIS Compliance	Format Identification	R1C4 Must
RD-3585	The system shall have the capability to notify a user of the characterization error.	OAIS Compliance	Format Identification	R1C4 Must
RD-3962	If a user manually changes file format identification, characterization, or validation information, the system shall note that in metadata.	OAIS Compliance	Format Identification	R1C4 Must
RD-3963	The system shall have the capability to allow users to enter notes in metadata about a file format validation failure.	OAIS Compliance	Format Identification	R1C3 Must
RD-502	The system shall identify file type without using external signature (i.e. file extension).	OAIS Compliance	Format Identification	R1C3 Must
RD-1784	The system shall accept digital content and metadata.	OAIS Compliance	Ingest	R1C2 Must
RD-1785	The system shall create a SIP from submitted content and metadata.	OAIS Compliance	Ingest	R1C2 Must
RD-1924	The system shall have the capability to notify Content Evaluators that new content has been received by the system.	OAIS Compliance	Ingest	R1C3 Must
RD-205	The system shall provide the capability to ingest into FDsys a SIP that is aggregated in a ZIP file.	OAIS Compliance	Ingest	R1C4 Must
RD-219	The system shall verify that all mandatory metadata elements are present and valid in order for a SIP to be eligible for ingest into FDsys.	OAIS Compliance	Ingest	R1C2 Must
RD-245	The AIP shall contain a rendition of the publication in the format in which it was submitted	OAIS Compliance	Ingest	R1C2 Must
RD-310	The AIP shall incorporate all metadata elements from the SIP.	OAIS Compliance	Ingest	R1C2 Must
RD-3964	The system shall have the capability to reject SIPs based on configurable criteria.	OAIS Compliance	Ingest	R1C4 Must
RD-484	The system shall create AIPs from in-scope SIPs at ingest.	OAIS Compliance	Ingest	R1C2 Must
RD-491	The system shall provide a prompt to confirm that the user intends to submit the SIP to ingest.	OAIS Compliance	Ingest	R1C2 Must
RD-492	The system shall validate that SIPs conform to requirements for a system compliant SIP.	OAIS Compliance	Ingest	R1C2 Must
RD-493	The system shall reject SIPs that have not been ingested after a configurable period of time.	OAIS Compliance	Ingest	R1C2 Must
RD-494	The system shall verify that all metadata files are valid.	OAIS Compliance	Ingest	R1C2 Must
RD-495	The system shall verify that at least one digital object is present at ingest.	OAIS Compliance	Ingest	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-497	The system shall provide the capability to allow an authorized user to reject a non-conforming SIP.	OAIS Compliance	Ingest	R1C2 Must
RD-498	The system shall have the capability to direct exceptions to the ingest process to authorized users other than the submitter.	OAIS Compliance	Ingest	R1C2 Must
RD-499	The system shall provide the capability for authorized users to process SIPs to conform to SIP validation.	OAIS Compliance	Ingest	R1C4 Must
RD-500	The system shall provide the capability to notify authorized users that a SIP is nonconforming.	OAIS Compliance	Ingest	R1C2 Must
RD-501	The system shall provide the capability to notify authorized users of the reasons a SIP is nonconforming.	OAIS Compliance	Ingest	R1C2 Must
RD-143	The SIP for Harvested Content shall contain one or more rendition consisting of the original harvested digital objects.	OAIS Compliance	Package management	R1C4 Must
RD-147	The SIP for Converted Content shall contain, at a minimum, a rendition consisting of the digital object(s) as produced by the conversion process.	OAIS Compliance	Package management	R1C4 Must
RD-148	The SIP for converted Content shall support the inclusion of representation information and metadata describing the conversion process for each rendition.	OAIS Compliance	Package management	R1C4 Must
RD-204	The system shall provide the capability to aggregate the SIP into a ZIP file.	OAIS Compliance	Package management	R1C4 Must
RD-246	The system shall provide the capability for authorized users to add renditions of a publication to an AIP.	OAIS Compliance	Package management	R1C4 Must
RD-346	The ACP shall include copies of renditions from its corresponding AIP based on business rules.	OAIS Compliance	Package management	R1C4 Must
RD-356	The system shall provide the capability to include metadata files as required to support access and delivery	OAIS Compliance	Package management	R1C4 Must
RD-151	A content package shall contain one or more renditions of one publication	OAIS Compliance	Package Structure	R1C2 Must
RD-152	A content package that describes a publication which only exists in tangible form shall contain a surrogate digital object that describes its tangible expression.	OAIS Compliance	Package Structure	R1C4 Must
RD-164	A SIP shall contain a METS file named sip.xml.	OAIS Compliance	Package Structure	R1C2 Must
RD-170	A content package shall contain one or more metadata files associated with the content.	OAIS Compliance	Package Structure	R1C2 Must
RD-173	Metadata files in a SIP shall be encoded in XML.	OAIS Compliance	Package Structure	R1C2 Must
RD-1822	The system shall provide the capability to record Structure Information of the content.	OAIS Compliance	Package Structure	R1C2 Must
RD-192	The folder structure of the digital objects in a rendition folder of a content package shall be recorded in the METS file.	OAIS Compliance	Package Structure	R1C2 Must
RD-203	The system shall provide the capability to aggregate all the files and directories in a SIP into a single package.	OAIS Compliance	Package Structure	R1C2 Must
RD-251	A rendition subdirectory in a content package shall contain subdirectories when necessary to support the original directory structure of the rendition.	OAIS Compliance	Package Structure	R1C2 Must
RD-261	The system shall provide the capability to add content to a content package independent of the content's digital format.	OAIS Compliance	Package Structure	R1C2 Must
RD-268	An AIP shall contain a METS file named aip.xml.	OAIS Compliance	Package Structure	R1C2 Must
RD-269	The METS file in a content package shall contain an inventory of all the content files in the package.	OAIS Compliance	Package Structure	R1C2 Must
RD-27	The system shall assemble content and metadata files into content packages that are compliant with open standards.	OAIS Compliance	Package Structure	R1C2 Must
RD-270	The METS file in a content package shall contain an inventory of all the metadata files in the package.	OAIS Compliance	Package Structure	R1C2 Must
RD-271	The METS file in a content package shall contain the relationships between the content files and metadata files.	OAIS Compliance	Package Structure	R1C2 Must
RD-275	The system shall retain submitted presentation information in the content package.	OAIS Compliance	Package Structure	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-289	The AIP shall contain the aip.xml at the top level of the AIP directory structure.	OAIS Compliance	Package Structure	R1C2 Must
RD-293	The order of the digital objects in a rendition folder shall be recorded in the METS file.	OAIS Compliance	Package Structure	R1C2 Must
RD-300	Metadata files in an AIP shall be encoded in XML.	OAIS Compliance	Package Structure	R1C2 Must
RD-301	Metadata files in a content package shall conform to a schema, DTD, or input standard that is registered in the FDsys Metadata Schema Registry.	OAIS Compliance	Package Structure	R1C2 Must
RD-312	The system shall support the capability for the content package to contain one or more administrative metadata files about each rendition.	OAIS Compliance	Package Structure	R1C2 Must
RD-316	Content packages shall have the capability to include Preservation Description Information (PDI) about each rendition.	OAIS Compliance	Package Structure	R1C2 Must
RD-319	The system shall have the capability to include rights metadata about each rendition in a content package.	OAIS Compliance	Package Structure	R1C4 Must
RD-3248	The system shall have the capability to retrieve ACPs from Access Content Storage based on user request.	OAIS Compliance	Package Structure	R1C2 Must
RD-33	Each content file in a content package shall be associated with one or more metadata files.	OAIS Compliance	Package Structure	R1C2 Must
RD-337	A content package shall contain one content unit that may consist of one or more digital objects.	OAIS Compliance	Package Structure	R1C2 Must
RD-34	Each metadata file in a content package shall be associated with one or more content files.	OAIS Compliance	Package Structure	R1C2 Must
RD-353	METS files shall conform to METS version 1.5.	OAIS Compliance	Package Structure	R1C2 Must
RD-354	METS files shall conform to the GPO METS Profile version 1.0.	OAIS Compliance	Package Structure	R1C2 Must
RD-355	An ACP shall contain a METS file named ACP.xml	OAIS Compliance	Package Structure	R1C2 Must
RD-376	The system shall have the capability to include technical metadata about each rendition in a content package.	OAIS Compliance	Package Structure	R1C2 Must
RD-377	The system shall have the capability to include analog source metadata about each rendition in a content package.	OAIS Compliance	Package Structure	R1C4 Must
RD-74	The system shall refer to metadata files rather than embed data elements in the METS wrapper.	OAIS Compliance	Package Structure	R1C2 Must
RD-265	The system shall provide the capability for authorized users to access AIPs for the purpose of executing preservation processes on AIPs.	OAIS Compliance		R1C4 Must
RD-467	The system shall have the capability to perform integrity checking.	OAIS Compliance		R1C4 Must
RD-614	The system shall ensure content submitted is not changed by refreshment.	OAIS Compliance		R1C4 Must
RD-615	The system shall have the ability to verify that the refreshed file is authentic and faithful.	OAIS Compliance		R1C4 Must
RD-616	The system shall provide logs that record the results of refreshment processes.	OAIS Compliance		R1C4 Must
RD-617	The system shall have the ability to notify users of incomplete or unsuccessful refreshment processes.	OAIS Compliance		R1C4 Must
RD-618	The system shall have the ability to identify incomplete or unsuccessful refreshments processes.	OAIS Compliance		R1C4 Must
RD-619	The system shall have the ability to produce notification of incomplete or unsuccessful refreshments processes.	OAIS Compliance		R1C4 Must
RD-381	The system shall reference the unique ID of the corresponding AIP in the ACP	OAIS Compliance	Unique ID	R1C2 Must
RD-3965	The system shall reference the unique ID of the corresponding ACP in the AIP.	OAIS Compliance	Unique ID	R1C2 Must
RD-3966	The system shall have the capability to create and assign a unique ID to metadata files.	OAIS Compliance	Unique ID	R1C2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-455	The system shall create and assign a unique ID to each content file.	OAIS Compliance	Unique ID	R1C2 Must
RD-457	The system shall create and assign a unique ID to each granule.	OAIS Compliance	Unique ID	R1C2 Must
RD-458	The system shall have the capability to create and assign a unique ID to jobs.	OAIS Compliance	Unique ID	R1C2 Must
RD-459	The system shall populate the Identifier field in the corresponding MODS record with the content package unique ID.	OAIS Compliance	Unique ID	R1C2 Must
RD-650	Unique ID shall be human-readable.	OAIS Compliance	Unique ID	R1C2 Must
RD-651	Unique ID shall be expressible in XML ID.	OAIS Compliance	Unique ID	R1C2 Must
RD-652	Unique ID shall be an alphanumeric identifier (ANI).	OAIS Compliance	Unique ID	R1C2 Must
RD-656	Unique ID shall have the capability to include the numbers 0-9 and letters A-Z (minus I and O).	OAIS Compliance	Unique ID	R1C2 Must
RD-658	Unique ID shall be unique.	OAIS Compliance	Unique ID	R1C2 Must
RD-709	The system shall create and assign a unique ID to each SIP.	OAIS Compliance	Unique ID	R1C2 Must
RD-711	The AIP shall inherit the unique ID from the SIP.	OAIS Compliance	Unique ID	R1C2 Must
RD-712	The ACP shall inherit the unique ID from the SIP if an AIP is not created.	OAIS Compliance	Unique ID	R1C2 Must
RD-713	The system shall create and assign a unique ID to each ACP if a unique ID is not inherited from the SIP.	OAIS Compliance	Unique ID	R1C2 Must
RD-716	The system shall record unique IDs in metadata.	OAIS Compliance	Unique ID	R1C2 Must
RD-720	The system shall allow the capability for an authorized user to retrieve content and information about the content associated with a unique ID.	OAIS Compliance	Unique ID	R1C2 Must
RD-3932	The system shall exclude records from being sent to the ILS based on a set of configurable criteria.	OAIS Compliance		R2 Must
RD-3934	The system shall maintain a dynamic list of serials and series based on cataloging records from the ILS.	OAIS Compliance		R2 Must

3.9 PERSISTANT NAME FEATURE GROUP REQUIREMENTS

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-726	The system shall assign persistent names to all in-scope published versions.	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-727	Persistent name shall not conflict with other identifiers within FDsys.	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-729	The system shall follow the guidelines outlined in Persistent Identification: A Key Component Of An E-Government Infrastructure. CENDI Persistent Identification Task Group (March 10, 2004).	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-730	The system shall follow the guidelines outlined in Interagency Committee on Government Information Recommendations to the Office of Management and Budget (December 17, 2004).	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-731	The system shall comply with RFC 1737 Functional Requirements for Uniform Resource Names (December 1994).	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-732	The system shall comply with RFC 2141 URN Syntax (May 1997).	Persistent Name	Persistent Name Assignment	R1C3 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-733	The system shall comply with RFC 2396 Uniform Resource Identifiers (URI): Generic Syntax (August 1998).	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-736	The system shall support the persistent name assigned by GPO as the definitive persistent name.	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-737	The system shall allow GPO to designate other systems or agencies to become recognized GPO naming authorities.	Persistent Name	Persistent Name Assignment	R1C4 Must
RD-738	The system shall assign persistent names that are location independent.	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-739	The system shall assign persistent names that are protocol independent.	Persistent Name	Persistent Name Assignment	R3 Must
RD-740	Persistent names shall be unique.	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-741	The system shall have the capability to assign intelligent persistent names.	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-742	The system shall have the capability to assign predictable persistent names.	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-745	The system shall have the capability to record the date and time of persistent name creation in metadata.	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-747	The system shall have the capability to create reports about persistent name management.	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-753	The system shall support one persistent name per publication	Persistent Name	Persistent Name Assignment	R1C3 Must
RD-2269	The system shall provide the capability for public users to use persistent names to access content.	Persistent Name	Persistent Name Resolution	R1C3 Must
RD-734	The system shall support interoperability across different naming systems to allow one system to access a resource within another.	Persistent Name	Persistent Name Resolution	R3 Should
RD-735	The system shall accommodate OpenURL syntax to enable federated searching.	Persistent Name	Persistent Name Resolution	R3 Must
RD-755	The system shall use a resolution system to locate and provide access to content with persistent names.	Persistent Name	Persistent Name Resolution	R1C3 Must
RD-756	The resolution process shall resolve an assigned name to a publication or the publication metadata.	Persistent Name	Persistent Name Resolution	R1C3 Must
RD-757	The resolution process shall allow for persistent name recognition within standard browsers.	Persistent Name	Persistent Name Resolution	R1C3 Must
RD-758	The system shall have the capability to support distributed persistent naming and resolution at the local and global level.	Persistent Name	Persistent Name Resolution	R1C3 Must
RD-759	The system shall support resolution of a single persistent name to multiple distributed locations.	Persistent Name	Persistent Name Resolution	R1C4 Should / R2 Must
RD-760	The system shall be able to identify and resolve to multiple identical copies of a resource at multiple locations through a single persistent name.	Persistent Name	Persistent Name Resolution	R1C4 Should / R2 Must
RD-761	The system shall support resolution of a single persistent name to multiple content versions.	Persistent Name	Persistent Name Resolution	R1C4 Should / R2 Must
RD-762	The system shall determine the most appropriate rendition based on attributes of the request.	Persistent Name	Persistent Name Resolution	R1C4 Should / R2 Must

3.10 PRESERVATION AND PROCESSING FEATURE GROUP REQUIREMENTS

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-2867	The system shall record order numbers in metadata.	Preservation and Processing		R2 Must
RD-2890	The system shall provide the capability to add metadata specifically for GPO sales purposes (e.g., book jacket art, reviews, summaries).	Preservation and Processing		R2 Could
RD-100	The system shall provide a GUI interface for users to manage the Schema Registry	Preservation and Processing		R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-1023	The system shall log all version history.	Preservation and Processing		R2 Must
RD-1024	The version history log shall be incorporated into the package's metadata.	Preservation and Processing		R2 Must
RD-1030	The system shall apply rules for version triggers.	Preservation and Processing		R2 Must
RD-1031	The system shall apply rules for version triggers to groups of related content as defined in the GPO document Version Control in Relation to Government Documents.	Preservation and Processing		R2 Must
RD-1032	Authorized users shall be able to modify rules for version triggers.	Preservation and Processing		R2 Must
RD-1034	The system shall detect modifications to content as a version trigger	Preservation and Processing		R2 Must
RD-1035	The system shall detect changes to the "last updated" data provided within the document as a version trigger	Preservation and Processing		R2 Must
RD-1036	The system shall detect changes to a flat date provided within the document as a version trigger	Preservation and Processing		R2 Must
RD-1037	The system shall detect changes to a publication's title as a version trigger	Preservation and Processing		R2 Must
RD-1038	The system shall detect changes to a publication's edition statement and/or metadata as a version trigger.	Preservation and Processing		R2 Must
RD-1039	The system shall detect changes in the issuing agency of a publication as a version trigger	Preservation and Processing		R2 Must
RD-1040	The system shall detect changes in file size or format as a version trigger	Preservation and Processing		R2 Must
RD-1041	The system shall detect changes in the publication's numbering scheme as a version trigger.	Preservation and Processing		R2 Must
RD-1042	The system shall detect notification of the publisher (i.e., issuing agency) as a version trigger.	Preservation and Processing		R2 Must
RD-1043	The system shall provide the capability to notify users when version triggers have been activated.	Preservation and Processing		R2 Must
RD-1045	The system shall provide the capability to notify designated authorized users when a version cannot be determined.	Preservation and Processing		R2 Must
RD-1047	The system shall determine if version identifiers are present in content packages.	Preservation and Processing		R2 Must
RD-1054	The system shall determine and record relationships between versions.	Preservation and Processing		R2 Must
RD-1055	The system shall establish links to related documents identified through version information in metadata.	Preservation and Processing		R2 Must
RD-1056	The system shall make links to related documents permanently available.	Preservation and Processing		R2 Must
RD-1057	The system shall be able to render relationship information so that it is human-readable.	Preservation and Processing		R2 Must
RD-1059	The system shall have the capability to notify users which version of content they are accessing.	Preservation and Processing		R2 Must
RD-1060	The system shall have the capability to notify users of the number of available versions of selected content.	Preservation and Processing		R2 Must
RD-1061	The system shall have the capability to notify users that they are not viewing the latest available version of selected content.	Preservation and Processing		R2 Must
RD-1062	The system shall have the capability to notify users of the relationship between the version of the content they are accessing and the latest version.	Preservation and Processing		R2 Must
RD-1063	The system shall have the capability for users to view the difference in the content between versions.	Preservation and Processing		R3 Must
RD-1064	The system shall have the capability to notify users that access to a version is restricted.	Preservation and Processing		R2 Must
RD-113	The system shall have the capability to receive and record existing metadata from sources external to the system.	Preservation and Processing		R3 Must
RD-114	The system shall have the capability to receive existing MARC metadata from sources external to the system."	Preservation and Processing		R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-115	The system shall have the capability to record existing MARC metadata from sources external to the system."	Preservation and Processing		R2 Must
RD-116	The system shall have the capability to receive existing COSATI metadata from sources external to the system."	Preservation and Processing		R3 Must
RD-117	The system shall have the capability to record existing COSATI metadata from sources external to the system."	Preservation and Processing		R3 Must
RD-127	The system shall provide the capability to transform metadata from one standard to another prior to exporting it.	Preservation and Processing		R2 Must
RD-130	The system shall have the ability to create metadata meeting the requirements of one or more schema.	Preservation and Processing		R2 Must
RD-133	The system shall provide the capability to extract metadata from content.	Preservation and Processing		R2 Must
RD-144	The metadata for harvested content in the SIP shall consist of representation information, documentation of harvest & transformation(s), submission level metadata for each rendition.	Preservation and Processing		R2 Must
RD-175	The SIP specified in this document shall apply to all content types specified and accepted by FDsys: converted, deposited and harvested.	Preservation and Processing		R2 Must
RD-1787	The system shall to be able to accept, store, and deliver encrypted files.	Preservation and Processing		R2 Could
RD-1814	The system shall support the capability to record additional content identifiers in the future.	Preservation and Processing		R3 Must
RD-1826	The system shall record or ascertain the following information when available and applicable.	Preservation and Processing		R2 Must
RD-1902	The system shall record and ascertain other document elements in the future.	Preservation and Processing		R3 Must
RD-1910	The system shall record or ascertain additional audio elements in the future.	Preservation and Processing		R3 Must
RD-1911	The system shall record or ascertain elements relating to video.	Preservation and Processing		R2 Must
RD-1919	The system shall record or ascertain additional video elements in the future.	Preservation and Processing		R3 Must
RD-1920	The system shall provide the capability to support other formats in the future.	Preservation and Processing		R3 Must
RD-206	The system shall support the capability to aggregate the SIP into additional file formats in the future.	Preservation and Processing		R3 Must
RD-207	The system shall support the capability to ingest into FDsys a SIP that is aggregated in additional file formats in the future.	Preservation and Processing		R3 Must
RD-211	The system shall have the capability to store descriptive metadata in ONIX format in the SIP.	Preservation and Processing		R2 Must
RD-214	The system shall have the capability to store descriptive metadata in COSATI format in the SIP.	Preservation and Processing		R3 Must
RD-215	The system shall have the capability to store descriptive metadata in additional descriptive metadata formats in the future in the SIP.	Preservation and Processing		R3 Must
RD-2310	The system shall provide the capability to use GPOs ILS to access metadata repositories not resident within the system.	Preservation and Processing		R2 Must
RD-2320	The system shall provide the capability for GPO to manage access to content packages according to GPO business rules.	Preservation and Processing		R2 Must
RD-2389	The system shall provide the capability for GPO to customize what information is collected during user registration.	Preservation and Processing		R2 Must
RD-2393	The system shall provide the capability to collect information identifying the individual as a member of a user class during registration (e.g., agency, department, office, library, depository number, company, contractor code).	Preservation and Processing		R2 Must
RD-2397	The system shall provide the capability to collect proof of identity information from the user during registration.	Preservation and Processing		R2 Must
RD-2398	The system shall provide the capability to collect authority to publish information from the user during registration.	Preservation and Processing		R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-244	An AIP shall only be created for SIPs that contain a publication that is in scope for GPO's dissemination programs.	Preservation and Processing		R2 Must
RD-2875	The system shall support the creation of ONIX metadata	Preservation and Processing		R2 Must
RD-2876	The system shall support the creation of ONIX metadata from existing metadata.	Preservation and Processing		R2 Must
RD-2882	The system shall provide the capability to acquire and integrate metadata from external sources.	Preservation and Processing		R2 Must
RD-2888	System shall record the change history of cataloging metadata.	Preservation and Processing		R2 Must
RD-2923	The system shall support interactive processes so users can create reference tools.	Preservation and Processing		R2 Should
RD-2925	The system shall interface with, and allow full functionality of, the GPO Integrated Library System.	Preservation and Processing		R2 Must
RD-2926	The system shall be compliant with NISO and ISO standards commonly used in the information industry.	Preservation and Processing		R2 Must
RD-2927	The system shall be compliant with NISO standard Z39.2 - Information Interchange Format	Preservation and Processing		R2 Must
RD-2928	The system shall be compliant with NISO standard Z39.9 - International Standard Serial Numbering-ISSN	Preservation and Processing		R2 Must
RD-2929	The system shall be compliant with NISO standard Z39.29 - Bibliographic References	Preservation and Processing		R2 Must
RD-2930	The system shall be compliant with NISO standard Z39.43 - Standard Address Number (SAN) for the Publishing Industry	Preservation and Processing		R2 Must
RD-2931	The system shall be compliant with NISO standard Z39.50 - Information Retrieval: Application Service Definition & Protocol Specification	Preservation and Processing		R2 Must
RD-2932	The system shall be compliant with NISO standard Z39.56 - Serial Item and Contribution Identifier (SICI)	Preservation and Processing		R2 Must
RD-2933	The system shall be compliant with NISO standard Z39.69 - Record Format for Patron Records	Preservation and Processing		R2 Must
RD-2934	The system shall be compliant with NISO standard Z39.71 - Holding Statements for Bibliographic Items	Preservation and Processing		R2 Must
RD-2935	The system shall be compliant with NISO standard Z39.85 - Dublin Core Metadata Element Set.	Preservation and Processing		R2 Must
RD-2936	The system shall support commonly used cataloging standards.	Preservation and Processing		R2 Must
RD-2952	The system shall support the creation of ONIX records.	Preservation and Processing		R2 Must
RD-2953	The system shall provide the capability to support search of GPO local data elements that identify unique attributes of the FDLP (e.g., GPO Superintendent of Documents (SuDocs) classification number, Item number, Depository Library number).	Preservation and Processing		R2 Must
RD-309	The system shall have the capability to store descriptive metadata in additional descriptive metadata formats in the future in the AIP.	Preservation and Processing		R3 Must
RD-328	The system shall provide the user the capability to alter the length of time to retain an ACP in the system.	Preservation and Processing		R2 Must
RD-35	The system shall support the capability to transform the binding file of the content package into other formats.	Preservation and Processing		R3 Must
RD-3515	The system shall provide the capability to add new versions of input standards to the Schema Registry.	Preservation and Processing		R2 Must
RD-3516	The system shall provide the capability to remove input standards from the Schema Registry.	Preservation and Processing		R2 Must
RD-3539	The system shall copy the technical metadata included with in a digital still image file to an MIX metadata file to be stored in the package	Preservation and Processing		R2 Must
RD-3540	The system shall copy the technical metadata imbedded in a digital still image file to an MIX metadata file to be stored in the package	Preservation and Processing		R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3568	The system shall evaluate digital objects for validity (i.e., well-formed and it meets additional semantic-level requirements) where such semantic-level requirements have been specified in FDsys.	Preservation and Processing		R2 Must
RD-3569	The system shall record results of file format validation in metadata as valid, tolerable (i.e., not affecting the ability to preserve the digital object), or downgraded (i.e., reducing the ability to preserve the digital object beyond bit level).	Preservation and Processing		R2 Must
RD-3574	The system shall note digital object inhibitors (i.e. features of the object that inhibit access, use, or migration) in metadata.	Preservation and Processing		R2 Must
RD-3575	The system shall note the function (e.g., All Content, Function: Play, Function: Print) impaired by a digital object inhibitor, where it is possible to automatically discern.	Preservation and Processing		R2 Must
RD-3579	The system shall copy the technical metadata imbedded in a digital still image file into a MIX metadata file to be stored in the package.	Preservation and Processing		R2 Must
RD-3586	The system shall copy an objects format-specific technical information TBS to technical metadata.	Preservation and Processing		R2 Must
RD-369	The system shall support the capability to use additional descriptive metadata formats in the future to support access to publications.	Preservation and Processing		R3 Must
RD-434	The system shall provide the capability to support the Open Archives Initiative Metadata Harvesting Protocol version (TBD-434A).	Preservation and Processing		R3 Must
RD-488	The system shall have the capability to transform textual content metadata into XML.	Preservation and Processing		R2 Must
RD-489	The system shall support the capability to conform to future requirements for SIP validation.	Preservation and Processing		R3 Must
RD-513	The system shall manage preservation processes, including scheduled assessments and resulting actions, based on the attributes of the digital objects and apply the specified processes.	Preservation and Processing		R2 Must
RD-515	The system shall maintain the integrity of content throughout preservation processes.	Preservation and Processing		R2 Must
RD-516	The system shall ensure content is fully intelligible and unchanged in meaning and representation, compared to the original AIP, when a digital object goes through preservation processes	Preservation and Processing		R2 Must
RD-517	The system shall preserve essential behaviors of digital content when a digital object goes through a preservation process.	Preservation and Processing		R2 Must
RD-518	The system shall maintain content functionality associated with content presentation when a digital object goes through a preservation process.	Preservation and Processing		R2 Must
RD-519	The system shall preserve significant properties and attributes of digital content as a digital object goes through a preservation process.	Preservation and Processing		R2 Must
RD-520	The system shall maintain content structure when a digital object goes through a preservation process.	Preservation and Processing		R2 Must
RD-521	The system shall maintain content structure when a digital object goes through a preservation process.	Preservation and Processing		R2 Must
RD-522	The system shall maintain hyperlinks to content within the target document when a digital object goes through a preservation process.	Preservation and Processing		R2 Must
RD-523	The system shall have the capability to notify users that they are leaving GPO's website when a user selects a hyperlink that takes them to an external site.	Preservation and Processing		R2 Must
RD-526	The system shall be capable of scheduling or executing preservation processes on individual AIPs or on selected groups of archival content.	Preservation and Processing		R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-527	The system shall be capable of scheduling preservation processes on individual AIPs.	Preservation and Processing		R2 Must
RD-528	The system shall be capable of scheduling preservation processes on selected groups of archival content.	Preservation and Processing		R2 Must
RD-529	The system shall be capable of executing preservation processes on individual AIPs.	Preservation and Processing		R2 Must
RD-530	The system shall be capable of executing preservation processes on selected groups of archival content.	Preservation and Processing		R2 Must
RD-532	The system shall have the capability to transform digital object(s) into a digital object of another format.	Preservation and Processing		R3 Must
RD-620	The system shall have the ability to support emulation to preserve access to content.	Preservation and Processing		R2 Must
RD-621	The system shall have the ability to verify that the emulated file retains specified attributes and behaviors, i.e., is authentic and faithful.	Preservation and Processing		R2 Must
RD-622	The system shall support the transformation of AIPs into ACPs.	Preservation and Processing		R2 Must
RD-623	When a preservation process results in the creation of an additional rendition in an AIP, the system shall be capable of retaining the as-ingested rendition of the content in the AIP.	Preservation and Processing		R2 Must
RD-625	The system shall have the ability to assess ingested content and determine preservation processes based on the assessments.	Preservation and Processing		R2 Must
RD-626	The system shall allow scheduling of preservation assessments. Content attributes include, at a minimum, completeness, determination of structure, file format, file size, and fitness for use.	Preservation and Processing		R2 Must
RD-627	There shall be no limit set on the number or frequency of assessments.	Preservation and Processing		R2 Must
RD-628	The system shall have the ability to re-assess content stored in the system.	Preservation and Processing		R2 Must
RD-629	The system shall present a range of options to the Service Specialist for decision if the system is unable to make a determination.	Preservation and Processing		R3 Could
RD-631	The system shall support scheduling the automatic execution of preservation processes.	Preservation and Processing		R2 Must
RD-632	The system shall support batch Content Preservation of content.	Preservation and Processing		R2 Must
RD-633	The system shall support Content Preservation on an item-by-item basis.	Preservation and Processing		R2 Must
RD-634	The system shall maintain an audit trail of preservation processes.	Preservation and Processing		R2 Must
RD-635	The system shall support the ability for authorized users to request preservation processes.	Preservation and Processing		R2 Must
RD-642	The system shall capture or generate metadata which specifies the relationship of files resulting from preservation processes to their predecessors.	Preservation and Processing		R2 Must
RD-646	The system shall enable varying levels of access to preserved objects (e.g., limiting access to authorized user classes, or denying or restoring access to security-restricted content).	Preservation and Processing		R2 Must
RD-660	The system shall support granularity of any content based on the natural granularity boundaries of that content.	Preservation and Processing		R2 Must
RD-76	The system shall support the capability to employ additional established extension schema for expressing metadata in the future.	Preservation and Processing		R2 Must
RD-806	The system shall examine harvested content for the purpose of verifying the source of the harvested content.	Preservation and Processing		R2 Must
RD-807	The source (e.g., OriginInfo:publisher) of harvested content shall be recorded in metadata.	Preservation and Processing		R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-808	The system shall ensure that harvested content has not been altered or destroyed in an unauthorized manner as compared to the source from which the content was harvested, and information about content integrity should be recorded in metadata.	Preservation and Processing		R2 Must
RD-809	The system shall validate that harvested content has not been altered in an unauthorized manner as compared to the source from which the content was harvested.	Preservation and Processing		R2 Must
RD-810	The system shall validate that harvested content has not been destroyed in an unauthorized manner as compared to the source from which the content was harvested.	Preservation and Processing		R2 Must
RD-82	The system shall support the capability to employ additional input standards for expressing metadata in the future.	Preservation and Processing		R2 Must
RD-83	The system shall have the capability to employ Encoded Archival Description (EAD) version 2002 as an extension DTD.	Preservation and Processing		R2 Could
RD-84	The system shall have the capability to employ Text Encoding Initiative (TEI) TEI P4 DTD as an extension DTD.	Preservation and Processing		R2 Could
RD-85	The system shall have the capability to employ Data Document Initiative (DDI) version 2.1 as an extension DTD.	Preservation and Processing		R2 Could
RD-859	The system shall have the capability to ensure integrity of content within the system at a definable frequency.	Preservation and Processing		R2 Must
RD-86	The system shall have the capability to employ Federal Geographic Data Committee (FGDC) CSDGM Document Type Declaration as an extension DTD.	Preservation and Processing		R2 Could
RD-875	The system shall have the capability to verify that the electronic content is valid.	Preservation and Processing		R2 Must
RD-876	The system shall have the capability to verify that the electronic content is uncorrupted.	Preservation and Processing		R2 Must
RD-877	The system shall have the capability to verify that the electronic content is free of malicious code.	Preservation and Processing		R2 Must
RD-878	The system shall provide the capability to provide notification that a change has occurred to content within the system.	Preservation and Processing		R2 Must
RD-88	The system shall have the capability to employ MPEG 21 as an input standard.	Preservation and Processing		R2 Should
RD-880	The system shall provide the capability to notify designated users if content has been altered in an unauthorized manner.	Preservation and Processing		R2 Must
RD-881	The system shall provide the capability to notify designated users if content has been destroyed in an unauthorized manner.	Preservation and Processing		R2 Must
RD-89	The system shall have the capability to employ JPEG 2000 as an input standard.	Preservation and Processing		R2 Should
RD-90	The system shall have the capability to employ ONIX as an extension schema.	Preservation and Processing		R2 Must
RD-794	The system shall validate that deposited content has not been altered in an unauthorized manner during transmission from the authorized user to the system.	Preservation and Processing		R2 Must
RD-525	The system shall have the capability to produce DIPs which are interoperable with other OAIS-based repositories.	Preservation and Processing		R2 Must
RD-431	The system shall provide the capability to include information generated as a result of Content Originator ordering.	Preservation and Processing		R2 Must
RD-134	The system shall provide the capability for GPO to designate metadata elements as mandatory.	Preservation and Processing		R2 Must
RD-3930	The system shall enforce publication-specific metadata specifications when users modify content metadata.	Preservation and Processing		R2 Must
RD-3931	The system shall enforce granule-specific metadata specifications when users modify content metadata.	Preservation and Processing		R2 Must
RD-2894	The system will provide for display and output of brief citations.	Preservation and Processing		R2 Must

ID #	FDsys Requirement	Feature Group	Feature	Release
RD-3933	When a bibliographic record is merged in the ILS, the system shall merge the descriptive metadata in FDsys, subject to approval by an authorized user.	Preservation and Processing		R2 Must
RD-3512	The system shall have the capability for a authorized user to manage which extension schema maps to each input standard.	Preservation and Processing		R2 Must
RD-95	The system shall provide the capability to remove XML schema from the Schema Registry.	Preservation and Processing		R2 Must
RD-98	The system shall provide the capability to remove XML DTDs from the Schema Registry.	Preservation and Processing		R2 Must
RD-3940	The system shall copy the technical metadata imbedded in a digital still image that is in a published format to a MIX metadata file to be stored in the package for objects previously ingested into the system.	Preservation and Processing		R2 Must

APPENDIX A – FDSYS ACRONYMS AND ABBREVIATIONS

ACRONYM	DEFINITION
ABLS	Automated Bid List System
ACES	Access Certificates for Electronic Services
ACP	Access Content Package
ACS	Access Content Storage
ACSIS	Acquisition, Classification, and Shipment Information System
AES	Advanced Encryption Standard
AIP	Archival Information Package
AIS	Archival Information Storage
ANSI	American National Standards Institute
AP	Access Processor
ARK	Archival Resource Key
ASCII	American Standard Code for Information Interchange
ASP	Application Service Provider
BAC	Billing Address Code
BPEL	Business Process Execution Language
BPI	Business Process Information
BPS	Business Process Storage
CA	Certification Authority
CCSDS	Consultative Committee for Space Data Systems
CD	Compact Disk
CDN	Content Delivery Network
CDR	Critical Design Review
CD-ROM	Compact Disk Read Only Memory
CE	Content Evaluator
CFR	Code of Federal Regulations
CGP	Catalog of U.S. Government Publications
CMS	Content Management System
CMYK	Cyan, Magenta, Yellow, Black
CO	Content Originator
COOP	Continuity of Operations Plan
CP	Content Processor
CPI	Content Packet Information
CRC	Cyclic Redundancy Checks
CSV	Comma Separated Variable
DARD	Departmental Account Representative
DES	Data Encryption Standard
DIP	Dissemination Information Package
DNS	Domain Name System
DO	Digital Objects
DOI	Digital Object Identifier
DoS	Denial of Service
DPI	Dots Per Inch
DSR	Deployment System Review
DVD	Digital Versatile Disc
EAD	Encoded Archival Description
EAP	Estimate at Completion
EAP	Enterprise Application Platform
ePub	Electronic Publishing Section
FAQ	Frequently Asked Question
FBCA	Federal Bridge Certificate Authority
FDLP	Federal Depository Library Program
FICC	Federal Identity Credentialing Committee
FIFO	First In First Out
FIPS	Federal Information Processing Standard
FOB	Free on Board
FOIA	Freedom of Information Act

ACRONYM	DEFINITION
FTP	File Transfer Protocol
GAO	General Accounting Office
GAP	GPO Access Package
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GILS	Government Information Locator System
GPEA	Government Paperwork Elimination Act
GPO	Government Printing Office
HMAC	Key Hashed Message Authentication Code
HSM	Hardware Security Module
HTML	Hypertext Markup Language
Hz	Hertz
ID	Information Dissemination
IDD	Interface Design Description
IEEE	Institute of Electronics and Electrical Engineers
IETF	Internet Engineering Task Force
ILS	Integrated Library System
IP	Internet Protocol
IPR	Internal Progress Review
IPSEC	Internet Protocol Security
ISBN	International Standard Book Number
ISO	International Organization for Standardization
ISSN	International Standard Serial Number
IT	Information Technology
ITU	International Telecommunication Union
JDF	Job Definition Format
LDAP	Lightweight Directory Access Protocol
LOC	List of Classes
LPI	Lines Per Inch
MAC	Message Authentication Code
MARC	Machine Readable Cataloging
METS	Metadata Encoding and Transmission Standard
MMAR	Materials Management Procurement Regulation
MOCAT	Monthly Catalog of Government Publications
MODS	Metadata Object Descriptive Schema
MPCF	Marginally Punched Continuous Forms
NARA	National Archives and Records Administration
NB	National Bibliography
NC	National Collection
NDIIPP	National Digital Information Infrastructure and Preservation Program
NET	New Electronic Titles
NFC	National Finance Center
NIST	National Institutes of Standards and Technology
NLM	National Library of Medicine
OAI	Open Archives Initiative
OAI-PMH	Open Archives Initiative Protocol for Metadata Harvesting
OAIS	Open Archival Information Systems
OCLC	Online Computer Library Center
OCR	Optical Character Recognition
OLTP	On-line Transaction Processing
PCCS	Printing Cost Calculating System
PDA	Personal Data Assistant
PDF	Portable Document Format
PDI	Preservation Description Information
PDR	Preliminary Design Review
PICS	Procurement Information and Control System
PICSWEB	Procurement Information Control System Web
PKI	Public Key Infrastructure

ACRONYM	DEFINITION
PKITS	Public Key Interoperability Test Suite
PKIX	Public Key Infrastructure Exchange Group within the IETF
PKSC	Public-Key Cryptography Standard
POD	Print On Demand
PPR	Printing Procurement Regulation
PREMIS	PREservation Metadata: Implementation Strategies
PRONOM	Practical Online Compendium of File Formats
PTR	Program Tracking Report
PURL	Persistent URL
RAID	Redundant Array of Inexpensive Disks
RFC	Request for Comments
RGB	Red, Green, Blue
RI	Representation Information
RMA	Reliability, Maintainability, Availability
ROI	Return on Investment
RPPO	Regional Printing Procurement Office
RSA	Rivest, Shamir, Adleman
RVTM	Requirements Verification Traceability Matrix
SAML	Security Assertion Markup Language
SDR	System Design Review
Section 508	Section 508 of the Rehabilitation Act
SF	Standard Form
SGML	Markup Language
SHA	Secure Hash Algorithm
SIP	Submission Information Package
SMP	Storage Management Processor
SMS	Storage Management System
SPA	Simplified Purchase Agreement
SSL	Secure Socket Layer
SSP	System Security Plan
SSR	Software Specification Review
SuDocs	Superintendent of Documents
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
U.S.C.	United States Code
URL	Uniform Resource Locator
USGPO	United States Government Printing Office
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAIS	Wide Area Information Service
WAP	Wireless Application Protocol
WIP	Work in Process
WML	Wireless Markup Language
WMS	Workflow Management System
XML	eXtensible Markup Language
XMLDSIG	XML Signature
XMLENC	XML Encryption

APPENDIX B – GLOSSARY OF TERMS

Access: Services and functions that allow users to determine the existence, description, location, and availability of content, and request delivery of content and metadata.

Access aids: Tools and processes that allow users to locate, analyze, and order content and metadata.

Access Content Package (ACP): An information package that includes renditions of content and metadata that are optimized for access and delivery. See also **OAIS**

Access (or service) copy: A digital publication whose characteristics (for example a screen-optimized PDF file) are designed for ease or speed of access rather than preservation. See also **Derivative.**

Accessibility: Making tools and content available and usable for all users including those with disabilities; the degree to which the public is able to retrieve or obtain Government publications, either through the FDLP or directly through an digital information service established and maintained by a Government agency or its authorized agent or other delivery channels, in a useful format or medium and in a time frame whereby the information has utility.

Access Time: Time needed to confirm availability and location of requested data and start the process of returning data to the user.

Activity (Workflow): A unit of work performed by the system or a human within the workflow.

Alert: A notification sent to current user of the system via the GUI, e.g. pop-up.

Application Security: The protection of application data and systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats at the application level. See also **Security.**

Archival Information Package (AIP): An information package that includes all content, metadata and associated Preservation Description Information (PDI) needed to preserve the content in perpetuity. See also **OAIS**

Archive: A collection with related systems and services, organized to emphasize the long-term preservation of information.

Archive management - See **Preservation**.

Assessment: A pre-defined task that evaluates whether the original attributes of a digital object are correct. The purpose of this assessment is to provide with information needed to identify necessary preservation processes.

Attribute - A feature or characteristic; a property. Often used to describe the nature of electronic data. For example, a data value's attributes may include its data type (numeric, character, or date), range of values, or length.

Authentic: Describes content that is verified by GPO to be complete and unaltered when compared to the version approved or published by the Content Originator.

Authentication: Validation of a user, a computer, or some digital object to ensure that it is what it claims to be. In the specific context of the Future Digital System, the assurance that an object is as the author or issuer intended it. See also **Certification**.

Authenticity: The identity, source, ownership and/or other attributes of content are verified.

Automated Activity (Workflow): An activity conducted under the direct control of the system. Automated activities are performed by the system without requiring user interactions.

Availability: The degree to which information is obtainable through an intentional or unintentional provision of information and services.

Batch of Jobs: A set of Jobs selected by the user.

Batch of Workflow Instances: A set of Workflow Instances selected by the user.

Batch Submission: the ability to submit multiple files at once. This includes the capability to submit a folder(s) and maintain the directory structure of the files.

Beta Testing: Testing that validates that the system meets the mission and business needs for the capabilities allocated to that release that involve end users. This is the last test and is part of the decision for determining if the system is ready to be deployed to public. This testing involves real-world, internal exposure or operation to the system.

Born digital: In the Future Digital System context, digital objects, created in a digital environment, with the potential of multiple output products, including hard copy, electronic presentation, and digital media.

Browse: To explore a body of information on the basis of the organization of the collections or by scanning lists, rather than by direct searching.

Business Manager: A user class that makes policy decisions and develops business plans to meet Content Originator and End User expectations.

Business process: A set of one or more linked activities which collectively realize a business objective or policy goal, normally within the context of an organizational structure defining functional roles and relationships.

Business Process Execution Language (BPEL): An XML-based language to allow the sharing of tasks across a system.

Business process information: Administrative, non-content-specific information that is used or created by a business process.

Cataloging and indexing: Cataloging is comprised of the processes involved in constructing a catalog: describing information or documents to identify or characterize them, providing "entry points" (terms) peculiar to the information or document, e.g., author, title, subject, and format information, by which the information can be located and retrieved. The immediate product of cataloging is bibliographic records, which are then compiled into catalogs. Indexing is the process of compiling a set of identifiers that characterize a document or other piece of information by analyzing the content of the item and expressing it in the terms of a particular system of indexing. In GPO context, cataloging and indexing is the statutory term for the processes that produce the *Catalog of U.S. Government Publications* and its indexes. In the FDsys context, it is the process or results of applying bibliographic control to final published versions.

Certification: 1. Proof of verification, validation, or authority. Process associated with ensuring that a digital object is authentically the content issued by the author or issuer. 2. An assessment against a known standard.

Certified: Providing proof of verification of authenticity or official status.

Chain of custody: Physical possession or intellectual ownership of content. Provides details of changes of ownership or custody that are significant in terms of authenticity, integrity, and official status.

Collaboration: Allowing for multiple authors or content sources while maintaining digital asset and document control and provenance.

Collection: A GPO defined group of related content.

Collection plan or **Collection management plan:** The policies, procedures, and systems developed to manage and ensure current and permanent public access to remotely accessible digital Government publications maintained in the National Collection.

Composition: The process of applying a standard style or format to content.

Content: Information presented for human understanding. In FDsys, it is the target of preservation.

Content-Based Services: Value added services created from the processing, repurposing and delivering of content.

Content Delivery Network (CDN): An external service provider utilized for distributed storage and delivery.

Content Evaluator: A user class that determines whether submitted content is in scope for GPO's dissemination programs.

Content Management Lifecycle: the ability and processes used to create, ingest, process, manage, preserve, access, search, disseminate, and dispose content.

Content Originator: A user class that develops content, submits content to the system, and submits orders to GPO for services.

Content unit: Content matter defined and treated as a single entity. (e.g., publication, video, audio of the State of the Union Address)

Converted content: Digital content created from a tangible publication.

Cooperative Publication: Publications excluded from GPO's dissemination programs because they are produced with non-appropriated funds or must be sold in order to be self-sustaining. See 44 USC 1903.

Customization: Providing the ability for users to tailor options to meet their needs and preferences. Customization is not delivered dynamically (e.g., personalization); it is managed by users and is static until changed.

Dark archive (digital): The site or electronic environment wherein a second "copy" or instance of all master and derivative digital files, data, and underlying enabling code resides and is maintained, under the control of the managing organization or its proxy. The dark archive must be inaccessible to the general public. Access to the dark repository contents and resources ("lighting" the archive) is triggered only by a specified event or condition.

Dark archive (tangible): A collection of tangible materials preserved under optimal conditions, designed to safeguard the integrity and important artifactual characteristics of the archived materials for specific potential future use or uses. Eventual use of the archived materials ("lighting" the archives) is to be triggered by a specified event or condition. Such events might include failure or inadequacy of the "service" copy of the materials; lapse or expiration of restrictions imposed on use of the archives content; effect of the requirements of a contractual obligation regarding maintenance or use; or other events as determined under the charter of the dark archives.

Data Center: A facility containing enterprise-grade FDsys equipment.

Data mining: Discovery method applied to large collections of data, which proceeds by classifying and clustering data (by automated means) often from a variety of different databases, then looking for associations. Specifically applied to the analysis of use and user data for GPO systems, data mining includes the tools and processes for finding, aggregating, analyzing, associating, and presenting BPI and metadata to enhance internal and external business efficiencies.

Delivery time: Time needed to deliver requested data to user.

Deposited content: Content received from Content Originators in digital form.

Derivative: A alternate presentation of content, often optimized for a specific function (e.g., access, preservation, print). Language translations are not derivatives; they are a separate publication.

Device: Content delivery mechanisms for digital media, such as data storage devices (e.g., CD, DVD, etc.), wireless handheld devices, future media, and storage at user sites.

Digital media: An intermediary mechanism consisting of data storage devices to deliver content to users' storage or display devices.

Digital object: A discrete item that can be acted upon by the system. A digital object may be a form of content (e.g. an entire document or a granule).

Digital signature: A cryptographic code consisting of a hash, to indicate that data has not changed, encrypted with the public key of the creator or the signer.

Directory structure: the method used to organize the data within the directory (hierarchy).

Dissemination: The transfer from the stored form of a digital object in a repository to the client or user.

Dissemination Information Package (DIP)**:** An information package that consists of one or more renditions of content or metadata from an AIP or ACP that is delivered to users in response to a request. See also **OAIS**

Distribution: Applying GPO processes and services to a tangible publication and sending a tangible copy to depository libraries.

Document: A digital object that is the analog of a physical document, especially in terms of logical arrangement and use.

Draft: A preliminary version of content, not yet in its finalized form.

Dynamically Changed Workflow: Workflow process that is changed during executing.

Electronic presentation: The dynamic and temporary representation of content in digital format; strongly dependent upon file format and user's presentation device

Emulation: Replication of a computing system to process programs and data from an earlier system that is no longer is available.

End User: A user class that uses the system to access content and metadata.

Ensure: Instruction to make sure an action takes place.

Ephemeral: content that is outside of the scope of GPO's dissemination programs. This includes, but is not limited to envelopes, letterhead, and documents produced for an organization's internal use only.

External Activity: An activity that requires manual or automated processing external to FDsys.

Faithful digital reproduction: Digital objects that are optimally formatted and described with a view to their *quality* (functionality and use value), *persistence* (long-term access), and *interoperability* (e.g. across platforms and software environments). Faithful reproductions meet these criteria, and are intended to accurately render the underlying source document, with respect to its completeness, appearance of original pages (including tonality and color), and correct (that is, original) sequence of pages. Faithful digital reproductions will support production of legible printed facsimiles when produced in the same size as the originals (that is, 1:1).

FDLP Electronic Collection (EC): The digital Government publications that GPO holds in storage for permanent public access through the FDLP or are held by other institutions operating in partnership with the FDLP.

FDLP partner: A depository library or other institution that stores and maintains for permanent access segments of the Collection.

Final Published Version: Content in a specific presentation and format approved by its Content Originator for release to an audience. (See also **Government Publication; Publication**).

Fixity: the quality of being unaltered (e.g. "fixity of the text" refers to the durability of the printed word).

Format: In a general sense, the manner in which data, documents, or literature are organized, structured, named, classified, and arranged. Specifically, the organization of information for storage, printing, or display. The format of floppy disks and hard disks is the magnetic pattern laid down by the formatting utility. In a document, the format includes margins, font, and alignment used for text, headers, etc. In a database, the format comprises the arrangement of data fields and field names.

Format management -See **Preservation**.

Fugitive document: A U.S. Government publication that falls within the scope of the Federal Depository Library Program, but has not been included in the FDLP. These publications include tangible products such as ink-on-paper, microforms, CD-ROM, or DVDs. Fugitive documents most commonly occur when Federal agencies print or procure the printing of their publications on their own, without going through GPO.

Fulfillment: the processes related to the packaging and delivery of tangible goods for delivery.

Government publication: A work of the United States Government, regardless of form or format, which is created or compiled in whole or in part at Government expense, or as required by law, except that which is required for official use only, is for strictly operational or administrative purposes having no public interest or educational value, or is classified for reasons of national security.

Granularity: The degree or level of detail available within content in the system

Handle System: A comprehensive system for assigning, managing, and resolving persistent identifiers, known as "handles," for digital objects and other resources on the Internet. Handles can be used as Uniform Resource Names (URNs).

Hard copy: Tangible printed content.

Harvest: The identification and replication of content resident on web servers outside GPO's control.

Harvested content: Digital content within the scope of dissemination programs that is gathered from Federal agency Web sites.

History: A record of all system activities.

Hybrid: A package containing selected content from multiple information packages.

Information granularity: The degree or level of detail available in an information system. With reference to authentication, the level of detail or specificity (e.g., page, chapter, paragraph, line) to which veracity can be certified.

Ingest: The OAIS entity that contains the services and functions that accept SIPs from Producers, prepare Archival Information packages for storage, and ensure that information packages and their supporting descriptive information packages are established within OAIS.

In-Scope Content: Content that has been qualified to be included in one of GPO's content dissemination programs (Federal Depository Library Program, GPO Sales Program, International Exchange Program, Cataloging and Indexing Program, By-Law Program). Depending on the context of in-scope, this can mean one of any programs or specifically one program.

Integrity: Content has not been altered or destroyed in an unauthorized manner.

Integrity Mark: Conveys authentication information to users.

Intended Use: The designation that specific content delivery methods, file formats, or content presentations must be used for the purpose of legal reference.

Interoperability: Compatibility of workflow across standards (e.g., WFMC to BPEL) and, compatibility of workflow within a standard and across programming languages (e.g., Java and C++ working in WFMC).

Internal Activity: An activity conducted within FDsys.

Issue: A content unit that is part of a serial.

Item: A specific piece of material in a digital library or collection; a single instance, copy, or manifestation.

Job (Request for product or service): The business process information submitted by a user to request a product or service. It also includes the information concerning business and system processes to manage the request until fulfillment. A job may be associated with content and metadata to fulfill the request.

Job (Workflow): A set of manual and automated activities that produce a product or service. A job may use one or more workflows in order to produce a product or service. It can be a system process, not tied to content. It's tied to processes defined in a workflow application.

Light archive: A collection of tangible materials preserved under optimal conditions, designed to safeguard the integrity and important artifactual characteristics of the archived materials while supporting ongoing permitted use of those materials by the designated constituents of the archives. A light archive normally presupposes the existence of a dark archive, as a hedge against the risk of loss or damage to the light archives content through permitted uses. A light archive is also distinct from regular collections of like materials in that it systematically undertakes the active preservation of the materials as part of a cooperative or coordinated effort that may include other redundant or complementary light archives.

List of Jobs: A list of Jobs assigned to a particular user.

List of Workflow Instances: A list of Workflow Instances assigned to a particular user.

Localized presentation: Temporary representation of layout or structure on a user's local presentation device.

Locate (discover): The organized process of finding Web-based documents or publications that are within scope for a particular collection.

Manage: In Information Technology contexts, to add, modify, or delete content.

Manifestation: Form given to an expression of a work, e.g., by representing it in digital form.

Manual Activity (Workflow): An activity conducted in such a manner that the system cannot exert direct control. Manual activities are performed by users and require the system to wait for a user action to be completed.

Message: Communication between a process and the Workflow Management System.

Metadata: Metadata is a structured representation of information that facilitates interpretation, management, and location by describing essential attributes and significant properties. Metadata describes the content, quality, condition, or other characteristics of other data. Metadata describes how, when, and by whom information was collected, where it resides, and how it is formatted. Metadata helps locate, interpret, or manage. In current usage several types of metadata are defined: **descriptive**, which aids in locating information; **structural/technical,** which records structures, formats, and relationships; **administrative,** which records responsibility, rights, and other information for managing the information; and **preservation,** which incorporates elements of the other types specific to preserving the information for the long term.

Metadata Encoding and Transmission Standard (METS): An XML schema for encoding metadata associated with objects in a digital library.

Migration: Preservation of digital content where the underlying information is retained but older formats and internal structures are replaced by newer.

Modified workflow: Workflow process that is changed during process development or, not at runtime.

National Collection of U.S. Government Publications (NC): A comprehensive collection of all publications in scope for GPO's dissemination programs, content that should be in the Federal Depository Library Program, regardless of form or format. The NC will consist of multiple collections of tangible and digital publications, located at multiple sites, and operated by various partners within and beyond the U.S. Government.

Natural Granularity Boundaries: The structure that is set in a document's native format, including volumes, chapters, parts, sections, and paragraphs.

No-fee access: There are no charges to individual or institutional users for searching, retrieving, viewing, downloading, printing, copying, or otherwise using digital publications in scope for the FDLP.

Non-repudiation: Verification that the sender and the recipient were, in fact, the parties who claimed to send or receive content, respectively.

Notification: A message sent to a process or user, e.g. email, RSS, workflow instance.

Open Archival Information System Reference Model (OAIS): ISO 14721:2003 - A reference model for an archive, consisting of an organization of people and systems that has accepted the responsibility to preserve information and make it available for a designated community. The model defines functions, activities, responsibilities, and relationships within this archive, sets forth common terms and concepts, and defined component functions which serve as the basis for planning implementation.

Official: A version that has been approved by someone with authority.

Official content: Content that falls within the scope of the FDLP EC and is approved by, contributed by, or harvested from an official source in accordance with accepted program specifications

Official source: The Federal publishing agency, its business partner, or other trusted source.

Online Information eXchange (ONIX): A standard format that publishers can use to distribute electronic information about their books to wholesale, e-tail and retail booksellers, other publishers, and anyone else involved in the sale of books.

Online: A digital publication that is published at a publicly accessible Internet site.

Online dissemination: Applying GPO processes and services to an online publication and making it available to depository libraries and the public.

Open Requisition: The business process information (job) submitted by a user to request multiple products or services over a specific time period. Multiple jobs can be associated with an open requisition (e.g. Congressional Bills jobs are requested daily and each are associated to a fiscal year open requisition).

Operations Manager: A user class that develops and optimizes workflow processes and monitors the quality of system products.

Permanent Public Access (PPA): Government publications within the scope of the FDLP remain available for continuous, no-fee public access through the program.

Persistent Name: Provides permanence of identification, resolution of location, and is expected to be globally (e.g., internationally) registered, validated, and unique

Personalization: Dynamically tailoring options to match user characteristics, behavior, or preferences. Personalization is often implemented by analyzing data and predicting future needs.

Policy neutral: Refers to a system which is sufficiently flexible to accommodate changes in hardware, software, communication technology, processes, policy, personnel, locations, etc. without requiring major re-engineering or design changes. FDsys is envisioned as being responsive to policy, but it is not intended to be policy-constrained.

Pre-Ingest Bundle (PIB): Digital objects, related metadata, and BPI, gathered for transfer to a service provider in the event of a Content Originator request for a proof. After approval the PIB becomes a SIP for ingest.

Preliminary Composition: Preparatory representation of content format or structure

Presentation Device: A device that can present content for comprehension

Preservation: The activities associated with maintaining publications for use, either in their original form or in some verifiable, usable form. Preservation may also include creation of a surrogate for the original by a conversion process, wherein the intellectual content and other essential attributes of the original are retained. For digital materials, preservation includes the management of formats of information (including possible migration to newer versions), the storage environment, and the archival arrangement of information to facilitate preservation.

Preservation description information: Information necessary for adequate preservation of content information, including information on provenance, reference, fixity, and context. See also **OAIS**

Preservation master: A copy which maintains all of the characteristics of the original publication, from which true copies can be made.

Preservation master requirement: A set of attributes for a digital object of sufficient quality to be preserved and used as the basis for derivative products and subsequent editions, copies, or manifestations. Requirements for use, users, and state/condition/format of the source of the original object need to be noted.

Preservation processes: Activities necessary to keep content accessible and usable, including **Migration, Refreshment,** and **Emulation.**

Print on demand (POD): Hard copy produced in a short production cycle time and typically in small quantities.

Process: A formalized view of a "business process", represented as a coordinated (parallel and/or serial) set of process activities that are connected in order to achieve a common goal.

Provenance: The chain of ownership and custody which reflects the entities that accumulated, created, used, or published information. In a traditional archival sense, provenance is an essential factor in establishing authenticity and integrity.

Public Key Infrastructure (PKI): A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

Publication: Content approved by its Content Originator for release to an audience.
See also **Government publication**.

Publisher: The agencies that originate or create material for distribution or sale.

Pull: Downloading content on an as-needed basis. Content is made available for users to select and retrieve (“pull”) to local servers or computers. For example, currently users may be said to pull documents from GPO Access.

Push: Intentionally and specifically serving out information to a target recipients. Content is automatically sent (“pushed”) from GPO to a list of interested users. This is analogous to shipping a box of depository documents, only with electronic content instead of tangible copy.

Recipient: an authorized user or system process that is permitted to receive content per their user role and group.

Redundant Array of Inexpensive Disks (RAID): A set of different hardware storage configurations where multiple hard disk drives share and/or replicate data.

Reference tools: Finding aids, bibliographies, and other services to assist in the locating and use of information, often less formally organized than catalogs and indexes.

Refreshment: A preservation process for data extraction, cleaning and integration, and the triggering events of these activities.

Relationship: A statement of association between instances of entities. In PREMIS, the association(s) between two or more object entities, or between entities of different types, such as an object and an agent.

Render: To transform digital information in the form received from a repository into a display on a computer screen or other presentation to a user.

Rendition: Instance of a publication expressed using a specific digital format

Replication: Make copies of digital material for backup, performance, reliability, or preservation.

Representation Information: The information that maps a data object into more meaningful concepts. An example is the ASCII definition that describes how a sequence of bits (i.e., a Data Object) is mapped into a symbol.

Repository: A computer system used to store digital collections and disseminate them to users.

Requirements: In system planning, a requirement describes what users want and expect according to their various needs. Requirements draw a comprehensible picture to facilitate communications between all stakeholders in the development of a system, and outline the opportunities for development of successful products to satisfy user needs.

Response Time: The elapsed time between the end of an inquiry or demand on a computer system and the beginning of a response; for example, the length of the time between an indication of the end of an inquiry and the display of the first character of the response at a user terminal.

Rich media: Electronic presentation that uses enhanced sensory features such as images, video, audio, animation and user interactivity

Rider: Request by GPO, agency, or Congress that adds copies to a Request or C.O. Order placed by a publishing agency or Congress.

Search: Process or activity of locating specific information in a database or on the World Wide Web. A search involves making a statement of search terms and refining the terms until satisfactory result is returned. Searching is distinct from browsing, which facilitates locating information by presenting references to information in topical collections or other logical groupings or lists.

Section 508 - Section 508 of the Rehabilitation Act requires access to electronic and information technology procured by Federal agencies. The Access Board developed accessibility standards for the various technologies covered by the law. These standards have been folded into the Federal government's procurement regulations. http://www.access-board.gov/508.htm

Secondary dark archive (digital): Multiple “copies” or instances of the dark repository, maintained as assurance against the failure or loss of the original dark repository. The secondary dark repository must provide redundancy of content to the original dark repository, and the systems and resources necessary to support access to and management of that content must be fully independent of those supporting the original dark repository content.

Secondary service repository (digital): The secondary service archive is a “mirror” of the service archive, created to provide instantaneous and continuous access to all designated constituents when the access copy or service archive is temporarily disabled.

Security: The protection of systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. The measures and controls, including physical controls in conjunction with management, technical and procedural controls, that ensure the confidentiality, integrity and availability of information processed and stored by a system. See also **Application Security.**

Sender: an authorized user or system process that is permitted to submit content per their user role and group.

Serial Control: The activity of identifying and managing serials or series.

Service archive (digital)**:** The site or electronic environment wherein the derivative, or "use," files and metadata created from source objects (here, tangible government documents), as well as the software, systems, and hardware necessary to transmit and make those files and metadata accessible, are maintained for public display and use. The service repository contains the current and most comprehensive electronic versions of those source materials.

Service Provider: A user class that delivers the expected services and products.

Service Specialist: A user class that supports Content Originators and End users to deliver expected products and services.

Shared repository: A facility established, governed, and used by multiple institutions to provide storage space and, in some instances limited service for low-use library materials, primarily paper-based materials that do not have to be readily available for consultation in campus libraries.

Status: A representation of the internal conditions defining the state of a process or activity at a particular point in time.

Storage: The functions associated with saving digital publications on physical media, including magnetic, optical, or other alternative technologies.

Storage management - See **Preservation**.

Submission information package (SIP): The information package submitted by a Content Originator for ingest the system. See also **OAIS**

Subscription: An agreement by which a user obtains access to requested content by payment of a periodic fee or other agreed upon terms.

Submit: The action taken by an authorized user within FDsys to inform that a job, BPI, or content is approved to be processed by GPO or FDsys.

System: An organized collection of components that have been optimized to work together in a functional whole.

System metadata: Data generated by the system that records jobs, processes, activities, and tasks of the system.

Systems Administration: A user class that directly supports the use, operation, and integrity of the system

Tangible publication: Products such as ink-on-paper, microforms, CD-ROM, or DVDs, characterized by content recorded or encoded on a physical substrate.

Term Contract: The business process information (job) submitted by a user to request products or services over a specific time period with specific Service Providers. Multiple jobs can be ordered off term contract (e.g. a magazine printed once a week for a year). Term contracts include single award, multiple award, direct deal, and general usage.

Test Case: 1. A set of test inputs, execution conditions, and expected results developed for a particular objective, such as to exercise a particular program path or to verify compliance with a specific requirement. 2. Documentation specifying inputs, predicted results, and a set of execution conditions for a test item.
A document describing a single test instance in terms of input data, test procedure, test execution environment and expected outcome. Test cases also reference test objectives such as verifying compliance with a particular requirement or execution of a particular program path.

Transformation: A process that produces one or more content packages from another; e.g., SIPs are transformed into Access Content Packages (ACPs) and Archival Information Packages (AIPs).

Trusted content: Official content that is provided by or certified by a trusted source.

Trusted source: The publishing agency or a GPO partner that provides or certifies official FDLP content.

Unique Identifier: A character string that uniquely identifies digital objects, content packages and jobs within the system.

Use Case: A description of the behavior of a system or part of a system; a set of sequences or actions, including variants that a system performs to yield an observable result of value.

User acceptance testing: Testing that validates that the system meets GPO's mission and business needs for the capabilities allocated to that release, in order to expose issues before the system is released to a wider audience in beta testing. This testing involves real-world, internal exposure or operation to the system.

Validation: A process that ensures (e.g., proves) that data conforms to standards for format, content and metadata.

Variable Data Printing: A form of printing where elements such as text and images may be pulled from a database for use in creating the final package. Each printed piece can be individualized without stopping or slowing the press.

Verification: The process of determining and assuring accuracy and completeness. There is a known input and an expected output is confirmed (e.g. check).

Version: Unique manifestation of content.

Version control: The activity of identifying and managing versions.

Version information: Information stored in metadata that describes the relationship between versions.

Viable application: Application software which retains all of its original functionality.

Workbench: A set of available tools for each user class (e.g., Content Originator, End User) that are displayed on a graphical user interface. A user's role (e.g., cataloger, Federal depository librarian) determines which of the tools available to his or her class will be displayed on the graphical user interface.

Work in Progress (WIP): a collaborative workspace that allows Content Originators, Service Specialists, and Service Providers (SP) to submit, manage, and review content, metadata, and jobs prior to ingest. Content, metadata, and BPI (job information) are help in WIP storage until approved by the publisher.

Work Item: The representation of the work to be processed (by a workflow participant) in the context of an activity within a process.

Workflow: The automation of a business process, in whole or part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules.

Workflow Definition: A document that defines the activities, business rules, data flows, and personnel roles that specify how a GPO business process will be performed within FDsys.

Workflow Instance: A workflow definition that is being executed on a specific entities by a specific person.

Workflow Management System (WMS): A system that defines, creates, and manages the execution of workflows through the use of software, running on one or more workflow engines, which is able to interpret the process definition, interact with workflow participants and, where required, invoke the use of IT tools and applications.

Workflow Participant: A resource, human or computer tool/application, which performs the work represented in an activity.